InfoDOMAIN

ID

Spring Edition 2013

FRONT COVER: ***(Center) RDML Gretchen S. Herbert, commander of Navy Cyber Forces, encourages students and family members to get involved in Woodrow Wilson High School, Portsmouth, VA's Science, Technology, Engineering and Mathematics (STEM) program. (Photo by MC3(SW) Jacob Galito). See story on Page 20.***

Commander, Navy Cyber Forces
RDML Gretchen Herbert

Deputy Commander
Mr. Mark E. Kosnik

Public Affairs Officer
CDR Brenda Steele MacCrimmon

Deputy PAO/Editor-in-Chief
Mr. George D. Bieber

Managing Editor
Miss Jacky Fisher

Associate Editor &
Visual Information Specialist
Mr. Robin D. Hicks

Graphics & Layout Design Editor
MC3 (SW) Jacob D. Galito

InfoDomain is the professional magazine of Navy Cyber Forces that promotes the advancement of Information Dominance through an open exchange of better practices, tactics and current and future strategies to meet the global challenges of the information warfare domain.

Information contained in ***InfoDomain*** does not necessarily reflect the official views of the U.S. Government, the Department of Defense or the Department of the Navy. Editorial content is prepared by the Public Affairs Office of Navy Cyber Forces.

Articles for publication in ***InfoDomain*** should be submitted through the appropriate command representative. Security and policy review must be completed by submitting commands before submissions can be considered for publication. Address all correspondence to Editor in Chief, InfoDomain, Navy Cyber Forces, Public Affairs Office, Joint Expeditionary Base Little Creek - Fort Story, 2465 Guadalcanal Road, Suite 10, Virginia Beach, VA, 23459-3243; telephone (757) 417-7958 ext. 5, DSN 537-7958 ext. 5, FAX (757) 492-8702. Comments or queries may also be forwarded via e-mail to: **george.bieber@navy.mil**

CNO's Take: Wireless Cyberwar, EM Spectrum And Changing Navy

EDITOR'S NOTE: ***The author, ADM Jonathan Greenert, Chief of Naval Operations and most senior officer in the United States Navy, has increasingly emphasized the convergence between traditional electronic warfare -- long a strong suit of the Navy -- and the new arena of cyberspace. In this piece from AOL Defense magazine, the Admiral argues for treating "cyberspace and the electromagnetic spectrum" as a single domain of warfare on par with land, sea, air and space.***

An unmanned aircraft is returning to its ship when it suddenly loses control, plummeting 5,000 feet to the water and shattering on contact with the surface. Halfway around the world, the lighting at an airfield in North America flickers several times before finally going dark, forcing airliners to seek out an alternate airport to land. In a windowless control room, system administrators at a large international corporation are alerted to higher than normal internet traffic on their servers. Before they can intervene, files which hold the key to a new cancer-fighting drug are exfiltrated via the company's wireless network, placing 10 years of research and more than a billion dollars of investment at risk. These kinds of events, although uncommon, do happen - and they arise from our dependence on the electromagnetic (EM) spectrum.

The electromagnetic spectrum is an essential - and invisible - part of modern life. We unlock our car and control our television with remote controls, routinely communicate using smart phones, and avoid automobile or aircraft collisions with any number of electronic sensors. EM transmissions and cyberspace are also essential to modern warfare. Our military forces use wireless computer networks to coordinate operations and order supplies, use radars and sensors to locate each other and the enemy, and use electronic jammers to blind enemy radars or disrupt their communications.

With wireless routers or satellites part of almost every computer network, cyberspace and the EM spectrum now form one continuous environment. This environment is so fundamental to naval operations, and so critical to our national interests, that we must treat it on par with our traditional domains of land, sea, air and space. In fact, future conflicts will not be won simply by using the EM spectrum and cyberspace, they will be won within the EM spectrum and cyberspace. This will require changes to our operating concepts, military systems and - most importantly - a new way of thinking in our Navy.

From primitive tool to double-edged sword

Our use of the electromagnetic spectrum has changed dramatically since Heinrich Hertz discovered it in 1888. Right away, EM transmissions were used to communicate with ships at sea. But in 1922, Naval Research Laboratory scientists also used radio waves to detect a moving ship, creating radio detection and ranging, or radar. With war raging in Europe and East Asia, in 1939 the new technology was sent to USS New York for testing and experimentation. Based on the successful results, radars were soon installed throughout the Fleet and became pivotal to winning the war at sea.

Since World War II, the military pioneered new uses for the EM spectrum, from satellite navigation and radar jammers to short-range wireless networks and infrared missile seekers. Now computer processors and transmitters are inherent in almost all our shipboard equipment, and even mechanical systems such as gas turbine engines and guns are "on the grid."

The EM spectrum is also an integral part of our military and civilian computer networks. Just like in our homes or in a Starbucks, a wireless network provides mobility. We can keep far-flung forces, aircraft and ships connected with each other and commanders back home, but wireless systems also provide ways to access a network that is otherwise isolated from the wider internet. Navy forces have a unique opportunity to exploit (or be exploited by) this access because of their presence around the world and ability to closely approach opponents via the sea.

Commanding the electromagnetic & cyber environment

Official U.S. Navy Photo

ADM Jonathan Greenert
Chief of Naval Operations

America's key military advantage for the last twenty years has been our ability to sense and create a picture of our surroundings, then use that picture to control the air, sea, and undersea domains. The systems that build our operational picture have performed well in the relatively unchallenged EM environments of Iraq and Afghanistan, but in future conflicts that will not be the case.

Inexpensive jammers, signal detectors, computer processors and radios make it easier for unfriendly states, terrorists and criminals to manage their efforts while jamming our own ability to sense and communicate. Meanwhile, the number of users in the EM spectrum has grown dramatically over the last two decades. The result is an environment we struggle to sense,

. . . continued on Page 3

MyDOMAIN . . . continued from Page 2

understand and use in warfare. We need a concerted effort to harness the EM and cyber environment to give us a warfighting edge.

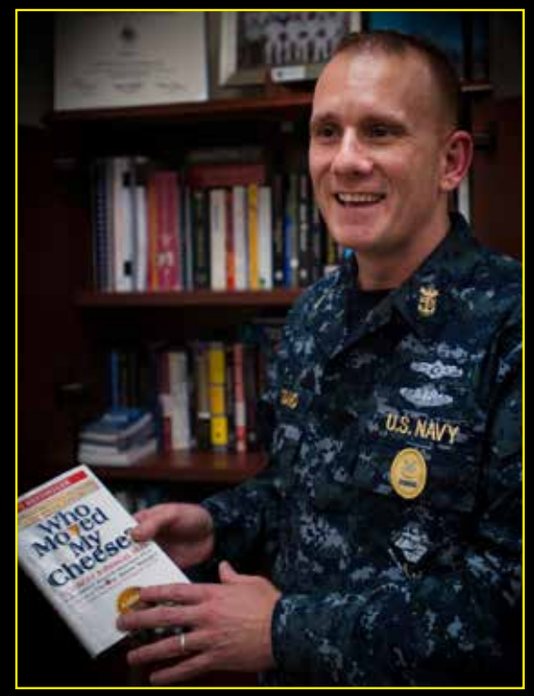
First, we will improve our awareness of the EM and cyber environments. We will detect and assess in real time what is happening in the EM and cyber environment, predict how the environment will react and use this knowledge to guide our own actions. Building this level of awareness will be challenging. Our tools for collecting and analyzing information in the EM and cyber environment are limited, and we lack the familiarity and understanding to take full advantage of the information we do have. To build better tools for sensing the EM and cyber environment, we will work closely with industry and academic researchers.

Second, we will employ agility in the EM spectrum and cyberspace. This will reduce our vulnerability to detection and maximize our ability to defeat jamming and deception. If our systems can shift frequency over a wide range, use shorter "burst" transmissions, employ small directional beams, or move applications between servers automatically in response to a sensed anomaly, our EM and cyber operations would be less predictable, harder to classify, and more difficult to counter or disrupt. One example of this is our "Integrated Topside" project, which uses modular, reconfigurable antennas in a ship's superstructure that can be alternatively employed as radars, listening devices, or radios.

Finally, we will change how we view the role of EM and cyber in warfare. EM and cyber systems and operators won't just support air, land, and space operations as they did in previous conflicts. Aircraft and ships will instead help get our EM and cyber capabilities into the fight. This will require developing the same "real-time" flexibility in planning and executing EM and cyber operations as we have today in the traditional "physical" domains.

Warfare in the EM spectrum and cyberspace is much more challenging than in other domains such as undersea or in the open ocean. The web and spectrum are crowded with civilian and commercial users who are rapidly developing and fielding new technologies. To take the high ground in this new environment, we will have to work with industry and fundamentally change our approach to operations and warfare. Most importantly, we will leverage those strengths that are impossible to reverse-engineer: the expertise and flexibility of our research base, our history of adaptation, and the skill and perseverance of our Sailors.

FORCE'S CORNER



Shipmates,

I would like to focus this article on a couple of recently released NAVADMINS. However, if you ever have questions about any NAVADMINS please ensure you bring this to the attention of your leadership. NAVADMIN 053/13 updated the requirements for Transition Goals, Plans, Success (GPS).

This program replaced the 20-year-old Transition Assistance Program (TAP) and is designed to strengthen, standardize and expand counseling and guidance for Active and Reserve Sailors separating from the Navy. Key components include pre-separation assessment, individual counseling and Department of Labor employment workshops. Please contact your respective career counselor for any questions related to GPS.

NAVADMIN 034/13 identified the Navy Office of Hazing Prevention (OPNAV N137) as the lead Navy entity for hazing policy. Hazing is defined as any conduct whereby a military member or members, regardless of service or rank, without proper authority causes another military member or members, regardless of service or rank, to suffer or be exposed to any activity which is cruel, abusive, humiliating, oppressive, demeaning or harmful. Hazing is contrary to our core values of honor, courage, and commitment and will absolutely not be tolerated. As a Navy, we must learn to embrace one another as a "Navy Family." I for one would never do anything to harm that family and I ask each of you to do the same. Please keep an eye out for this unfortunate activity and take appropriate action immediately.

NAVADMIN 012/13 introduced the Alcohol Detection Device (ADD). ADDs are one of many tools provided to commanders to complement other unit efforts to promote responsible use of alcohol and detect and deter alcohol abuse. The ADD program promotes safety, education and training, and awareness. I ask each of you who makes the choice to consume alcohol to do so responsibly and if you ever need a ride please contact a Shipmate, this includes myself. Thank you again for what each of you do every day in support to our nation, our Navy, and Navy Cyber Forces. The work you perform at NCF has a direct impact on the over 52,000 military and civilian members of the Information Dominance Corps.

Finally, a hearty Congratulations and Bravo Zulu to CTNC(SEL) McQueen assigned to NIOC Maryland for her recent selection as the 2012 CNO Shore Sailor of the Year. The entire IDC should be extremely proud of CTNC(SEL) and the impact this extremely dedicated Sailor is having on our Navy. Outstanding Shipmate!

FORCM Recommended Reading: "It's Your Ship" by Captain D. Michael Abrashoff

"Work Hard, Play Hard, but ALWAYS Do What is Right!"

Steven Giordano, Force Master Chief

Cloud Computing Memo Signed

On April 1, the Department of the Navy Chief Information Officer (DON CIO) signed out the memo, "Department of the Navy Approach to Cloud Computing." The memo states that to increase efficiency and achieve necessary cost savings, the department is moving forward to employ capable cloud computing solutions that meet mission and security requirements and provide best value. Unless a more cost effective solution is identified, the first step will be moving DON systems that host publically releasable information to commercial cloud service providers who meet all requirements.

The policy follows a recent pilot sponsored by the DON CIO with Amazon Web Services to move publicly accessible data to a commercial hosting environment. The Secretary of Navy's public-facing information portal is now hosted in the Amazon Web Services cloud infrastructure.

The innovative decision to host the data in a commercial cloud environment resulted from an analysis of several factors, the most important being the type of data stored in the portal, hosting costs and security requirements.

Read the memo:

"Department of the Navy Approach to Cloud Computing."

DON IM/IT 2013 Excellence & Electromagnetic Spectrum Awards Winners

The Department of the Navy Chief Information Officer is pleased to announce the winners of the 2013 DON IM/IT Excellence Awards and the John J. Lussier Electromagnetic Spectrum Leadership Award.

The annual DON IM/IT Excellence Awards recognize IM/IT projects, teams and individuals that have transformed the Navy and Marine Corps through information technology. Winners were selected for their superior leadership skills and innovative use of IM/IT to reduce, downscale, and downsize while not duplicating existing projects, systems or solutions. Through these efforts, they significantly improved the efficiency and effectiveness of the organization in delivering its mission.

The John J. Lussier Electromagnetic Spectrum Leadership Award is given to an individual who demonstrates superior achievement in Navy and Marine Corps electromagnetic spectrum management and use. This award is named for the former DON Principal Deputy Chief Information Officer who lost his courageous battle with cancer in June 2009. Lussier was an advocate for protecting the DON's equities in the electromagnetic spectrum and advanced the DON's strategic vision for spectrum.

Three individuals received the DON IM/IT Excellence Award and six Teams received the DON IM/IT Excellence Team Award.

For a listing of the 2013 winners, visit: http://www.doncio.navy.mil/ContentView.aspx?id=4398.

IA Workforce Baseline Certification Update

This alert provides notice of changes to the Department of Defense (DoD) 8570.01 Manual, "Information Assurance Workforce Improvement Program" baseline certifications. One certification has been added and two have been removed from the list.

The CompTIA Advanced Security Practitioner (CASP) certification has been approved as a DoD 8570 baseline certification. This certification is an international, vendor-neutral accreditation that proves competency in enterprise security; risk management; research and analysis; and integration of computing, communications, and business disciplines.

The Global Information Assurance Certification (GIAC) Security Expert (GSE) and GIAC Information Security Fundamentals (GISF) were removed from the DoD Approved 8570 Baseline Certifications list.

DoD 8570.01M Information Assurance (IA) baseline certifications are aligned to each category and level of the IA workforce. Personnel performing IA functions must obtain one of these certifications as required for their position, category/specialty, and level to fulfill the IA baseline certification requirement. Refer to Appendix 3 of 8570.01-M for further implementation guidance.

GSE and GISF were removed from the approved list on Jan. 25, 2013. Individuals who have either the GSE or GISF certification as a requirement for their current job will remain qualified until the GSE or GISF expires or until the individual changes to a position that requires a different certification. Once the GSE or GISF expires, a different certification may be required.

For more details visit the Information Assurance Support Environment (IASE) Certification web page at: http://iase.disa.mil/eta/iawip/content_pages/iabaseline.html.

Official U.S. Navy Photo

CTN1 Shannon McQueen

AND THE WINNER IS...

Chief of Naval Operations 2012 Shore Sailor of Year is Announced … Cryptologic Technician (Networks) 1st Class Shannon McQueen. The field was competitive, but a stellar member of the Information Dominance Corps (IDC) was the last Sailor standing for the Navy's 2012 Shore Sailor of the Year competition. McQueen will be meritoriously advanced to Chief Petty Officer May 16 at the Navy Memorial in Washington, DC.

McQueen's accomplishments and tenacious drive garnered praise from cyber leadership. "CNO made a terrific choice in selecting CTN1 McQueen the 2012 Shore SOY," said RDML Gretchen S. Herbert, commander, Navy Cyber Forces. "When talking with CTNC(sel) McQueen, her compassionate concern for the success and welfare of her Sailors comes through loud and clear -- and superbly complements her uncompromising dedication to mission accomplishment."

McQueen advanced to the final round in March after selecting as the U.S. Fleet Forces 2012 Shore Sailor of the Year. Extending his congratulations, VADM Michael Rogers, commander, U.S. Fleet Cyber Command/commander U.S. 10th Fleet said, "This selection is the culmination of exceptional dedication and a significant amount of hard work by CTN1 McQueen. She represents the best the IDC has to offer and clearly has maintained the highest levels of excellence and professionalism to earn this distinction."

A native of Crete, IL, McQueen entered the Navy September 1993. Joining as a non-designated Seaman, McQueen promptly advanced to Yeoman Third Class.

Looking for the next challenge, she cross-rated to Cryptologic Technician Maintenance (CTM). She graduated the six-month course with honors and followed that achievement with attending the Wide Area Network Maintenance Technician "C" school.

As a CTM1, McQueen was selected for direct conversion to CTN and transferred to Navy Cyber Defense Operations Command, Virginia Beach, VA. In 2007-2008, she attended the Basic and Intermediate Digital Network Analysis Course where she once again graduated with honors.

Currently McQueen is stationed at the Navy Information Operations Command, Maryland where she serves as Leading Petty Officer for two divisions, responsible for the professional and personal development of more than 200 Sailors. She is also the Command Managed Equal Opportunity Officer.

McQueen's Navy career crisscrossed the country and the globe. When she reflects on how her success was possible, she attributes it to two things. The trust from both Navy leaders and her Sailors to do the job and being guided by Navy core values, which, says McQueen, is "simply a reflection of what we do every day in the Navy."

"Petty Officer McQueen's conspicuous dedication to her team, her command, and our Navy is truly impressive and is an inspiration to us all," said Herbert. "Well done Chief!"

ADM Bill Gortney, commander, U.S. Fleet Forces, presents CTN1 Shannon McQueen, assigned to NIOC Maryland, with a helmsman clock after announcing her as the USFF 2012 Shore SOY. (Photo by MC1 Rafael Martie)

CTRC Joshua Gray, of Ontario, CA, rescued an injured man Jan. 6 at Walmart on the west end of Pensacola. Gray, an instructor at the Center for Information Dominance (CID) Unit Corry Station and certified emergency medical technician (EMT).

Family's Shopping Trip Turns Critical

Sailor utilizes medical training

Story & Photo by CTR1 Joshua Pugh, CID Public Affairs

PENSACOLA, FL-- An instructor at the Center for Information Dominance (CID) Unit Corry Station aided an injured man Jan. 6, while shopping with his family.

Chief Cryptologic Technician Collection Joshua Gray, of Ontario, CA, and his family were shopping at Walmart in Pensacola when he heard a girl scream.

"I looked up and saw her dad, basically pop to attention and fall straight back," Gray said. "His head was bleeding, and there was a pool of blood under him."

Gray, who reported on board CID Unit Corry Station in 2010 for instructor duty, received emergency medical training 10 years ago.

The man who had injured his head after falling to the floor and was bleeding profusely.

Gray, with assistance from another shopper, applied pressure to the back of his head to stop the bleeding and waited for the ambulance.

Gray believed the man might have suffered from a seizure, and that he seemed groggy when he regained consciousness.

"He really didn't know what was going on," Gray said. "I told him: 'Stay calm; you hit your head pretty hard.'"

Firefighters from Escambia County Fire Rescue Station 14 at nearby Pleasant Grove responded to the call.

In 2003, Gray received emergency medical technician (EMT) training and became a certified EMT. Inspired by that training, he pursued more medical qualifications and was recently selected for the Medical Enlisted Commissioning Program (MECP).

"The situation was chaotic," said Station 14 'C' Watch Lieutenant Bryan Caro, "but thanks to the Navy Chief, the chaos seemed to be under control."

Caro went on to say that, "Gray initiated first aid and C-spine precautions, and made sure the guy had an airway and didn't bleed to death before we got there, which was paramount."

Gray admitted, "That EMT training, combined with my Navy training, helped me stay calm and do what needed to be done."

Station 14 firefighters agreed that Gray's appropriate response helped make the situation better.

CID Unit Corry Station Commanding Officer Cmdr. L. Sung said she was not surprised by Chief Gray's immediate response to this situation, as he was recently selected to the MECP.

"His training served him well under this stressful situation, and he did the right thing at the right time," Sung said. "Chief Gray embodies the Navy's core values of honor, courage, and commitment, and I am proud to call him shipmate."

Illustration by MC3(SW) Jacob D. Galito, CYBERFOR Public Affairs

BUDGET & FLEET MODERNIZATION . . . IS THERE ENOUGH FOR C5ISR?

By CDR Brenda Steele MacCrimmon, CYBERFOR PAO

The President's 2014 portion of the budget for the Navy aims to follow-through on investments in improved technological modernization, operations and maintenance, (O&M), personnel and construction. It also seeks to preserve the Navy's forward-presence in support of the Pentagon's expanded strategy involving a shift of forces to the Pacific theater.

While there's still some budget uncertainty with the ongoing sequester and challenges remain regarding plans for certain types of maintenance, readiness and training, the recent passage of the Fiscal Year 13 appropriations bill has improved the Navy's overall budget outlook.

"It solved about half of my O&M problem" said RADM Joseph Mulloy, Deputy Assistant Secretary of the Navy, Budget. "I'm still sequestered a total of $4.5 billion but I'm not at an $8.6 billion deficit. With the CR and sequester, the Navy was tremendously short in O&M." [reprint from article: "Navy hauls in budget's largest share among services" by Kris Osborn on Thursday, April 11, 2013 in Naval Policy]

A few of the budget highlights: It increases cyberspace operations and electronic warfare capabilities will increase with the acquisition of 21 new EA-18G Growler aircraft and a carrier-based electronic warfare variant of the F/A-18F Super Hornet. The Office of the Secretary of Defense and the Navy also plan to grow the electronic jamming force, with the Navy picking that up essentially as a national force.

"Navy hauls in budget's largest share among services"

Even with the Navy receiving the largest portion of the baseline budget, allowing it to grow to a 300-ship Navy, Fleet modernization and how it's accomplished remains a concern. So, twice a year, a conference called the Navy C5I Modernization Conferences (NCMC) has participants focused on fielding plans through a week of discussions to properly address all of the C5I modernization priorities for that year.

"It's held with people at all the working levels, typically Captains and below, who openly discuss day-to-day issues related to Fleet modernization," said Navy Cyber Forces Fleet C5I Modernization Director John Undset. "The objective is to ensure that all platforms in a strike group are interoperable internally and externally."

"The objective is to ensure that all platforms in a strike group are interoperable internally and externally."

In between conferences, on a weekly basis, teams continue to liaise on Naval Sea Systems Command (NAVSEA) and Space and Naval Warfare Systems Command (SPAWAR) focused events to bring up ongoing issues.

"Some of these day-to-day challenges in the Fleet modernization process deal with the difficulty of aligning modernization between programs that have different rates of funding to accomplish that modernization," said Undset. "So, with Flag-level approval, we are in the initial stages of establishing a Variance Reduction Board (VRB) with the intent to align modernization initially with Program Executive Office (PEO C4I) systems into groups of interoperable capability packages." Undset summarized that the VRB's goals would be to increase interoperability, reduce numbers of baselines, which in turn, would reduce training requirements.

PEO C4I, which acquires, fields and supports C4I systems that extend across Navy, joint and coalition platforms, a baseline for all ships, is being established. Supported by SPAWAR and industry partners, PEO C4I annually completes more than 2,500 installations to maritime forces.

The new Consolidated Afloat Networks and Enterprise Services

. . . continued on Page 8

. . . continued from Page 7

(Top left) The Arleigh Burke-class guided-missile destroyer USS Milius (DDG 69) returns to homeport Naval Base San Diego after an eight-month independent deployment to the western Pacific.

(Above) Consolidated Afloat Networks and Enterprise Services (CANES) program technicians at the SPAWAR command prepare the program to be installed inside the USS Milius. (Photos by MC3 Karolina A. Martinez)

(Left) A signals switch rack destined for installation on the guided-missile destroyer USS McCampbell (DDG 85) awaits operational testing in SPAWAR Pacific's Network Integration and Engineering Facility (NIEF). The rack is one of many electronic components that make up the CANES modules currently being tested and installed on the USS Milius (DDG 69), USS McCampbell (DDG 85) and USS Chafee (DDG 90). (Photo by Rick Naystatt)

(CANES) represents a fundamental change in the Navy's way of acquiring networks as well as security capability. CANES is the future for the Fleet. It deploys a common network infrastructure, building on the mature Common Computing Environment (CCE) as well as Cross Domain Solution technologies to ensure a secure and reliable network infrastructure.

CANES will replace numerous duplicative networks, all provided through separate programs. It also provides greater capabilities, simplified installation and lower costs over its complete lifecycle.

CANES meets current and projected warfighter requirements, increases reliability and security, offers integrated voice, video, data and system management functions to reduce shipboard workload, and supports the US Navy's Maritime Strategy. More than 187 platforms afloat and Maritime Operational Centers ashore will have CANES installed. The guided missile destroyer USS Milius is currently undergoing installation of CANES, making it the first ship to receive the install.

"There's a period of modernization for each ship, it's a cycle," said Navy Cyber Forces C5I Forces Afloat Representative Doug Miller. "Our job is to provide the necessary upgrades and configurations to the warfighter that they need everyday to do their jobs."

"Bottom line," said Miller, "our purpose is to modernize our Fleet and the NCMC provides the framework to get this done."

Still, the time for the installs of CANES needs to speed up. "There's a schedule that needs to be maintained in order to get the Fleet properly modernized and in a timely manner," said Miller.

With CANES and the new common computing environment in place, security features get dramatically improved and many information assurance vulnerabilities are removed.

As new installs of any kind happen aboard ship, Undset pointed out an important protocol that should be in place.

"When PEO, SPAWAR and NAVSEA do installs aboard a ship, Sailors should be 'glued' to these installers because they are the experts who can tell you how to make a system perform optimally," said Undset. "Sailors need to get heavily engaged in the process."

Cyber Cat's Tips

Articles by Laurie Cummings, CISSP CYBERFOR IAM

Precaution & Judgement Key for Financial Decisions

It's that time of year again! The long winter chill has lifted, flowers are blooming and the fish - I mean, "Phish", are biting.

The IRS recently warned taxpayers during the filing season to beware of unsolicited emails that appear to be from either the IRS or an organization closely linked, such as the Electronic Federal Tax Payment System (EFTPS). Suspicious emails attempting to get your personal information should always be ignored.

TIP: The IRS and other financial institutions would never request personal or financial information via email, text message or social media sites. And neither would any valid professional organizations.

So be wary of emails asking for your log-in information, Social Security Number (SSN), or Tax Identification Number (TIN).

TIP: Never click on links in emails promising large sums of money, or urgently requesting you to log-in to verify your information. In order to help the Navy identify and mitigate these problems, do your part and quickly report suspicious e-mails.

If you are on a military installation and receive a suspicious e-mail, report it to your local Information Assurance Manager (IAM), or your chain of command immediately.

Twenty years ago was the "birth" of email as we know it. While the internet and the use of email systems have opened many doors and provided vast opportunities, we must always remain vigilant to ensure certain doorways remain secure. It is the responsibility of every Sailor and civilian to practice precaution and best judgment when accessing the internet with any type of device.

So, keep yourself safe and make sure when cyber criminals go phishing, you're the "one who got away".

Illustration by MC3(SW) Jacob D. Galito, CYBERFOR Public Affairs

EDITOR'S NOTE: ***Article taken from "On Cyber Patrol" & adapted to fit the Navy environment.***

Making Information Assurance a Priority, not an Afterthought

In only a few decades, our digital world has pushed our decision making process to extremes. As information flows faster, it forces us to react faster and solve problems faster. One could argue that in the military during a war that pressure is increased tenfold.

A military mind is extremely focused. Through intense training and situational drills, a Sailor is expected to react as prescribed by doctrine, to assess quickly a roadblock to mission success and go over it, around it, or through it as necessary.

For example, if a Sailor is ordered to move data from point A to B immediately, and the normal secured communication route is either down or slowed, a Sailor focused on successful completion of that task may bypass established communications and security procedures.

A person under this kind of pressure could think that there are times when rules and correct procedures appear to be more of a hindrance than a help. In their minds, consequences are something to be dealt with later. The flaw in that logic is that the consequences of bypassing Information Assurance (IA) procedures in wartime - hot or cold - could result in failed missions, compromised security, and lives unnecessarily put at risk.

The human mind is quick to adapt. As technology drives our thought processes, we will eventually be able to process information and decisions faster. Until that time, we need to take those critical few seconds that often spell the difference between doing it right or doing it wrong.

IA is too often an afterthought. It is imperative that it be at the front of every information transmission and storage choice and action. By taking those few extra seconds - more than enough time for a computer to do all your homework from kindergarten through high school - you can keep your IA decisions on track to protect yourself and your fellow Sailor.

Looking ahead to the Future

By CDR Brenda Steele MacCrimmon, CYBERFOR PAO

InfoDOMAIN magazine recently interviewed CISCO Systems' Senior Vice President of Advanced Security Initiatives, Greg Akers, who shared critical thoughts about the future of both military and civilian networking solutions.

When Akers joined CISCO in 1993, he started as a technical support engineer and eventually became a vice president for the company, whose primary focus was technology and security for its worldwide customers.

He was initially in charge of CISCO's information security team, and then, in 2002, Akers went a step further and formed the company's Global Government Solutions Group (GGSG) when the need for much better support to customers in the U.S. and abroad was identified.

When Akers attended a users' conference and asked one of the attending top executives, "How are we doing with servicing to USG customers," he was shocked at the exec's response. Akers was told that his company didn't have 'properly cleared' people to work within USG (U.S. Government) customer's special work spaces. Therefore, the CISCO employees could never actually see the network problems firsthand that the customers were facing on a daily basis. "USG customers would black out things on their network and we would work the issues from a distance," said Akers.

That's how GGSG was born. CISCO's engineering group began designing special products and adaptations for USG customers and several other clients. For the first time, the company also began offering alterations to many of its commercial products for special uses in the military. "We began developing adaptations for our intelligence customers worldwide for use in the field," said Akers.

"Believing that an infrastructure is secure because of its classification level is one very risky practice."

CISCO's market grew, and serious partnerships developed, which in turn helped aid military missions worldwide. The partnership eventually spawned products like the rugged-aided routers found aboard U.S. Navy ships for specific emerging crypto requirements.

Army Soldiers also started seeing the rugged-type devices available in their Humvees.

"It makes a military person's job easier because they can take advantage of commercial optimizations," according to Akers, "without specialized engineering."

'The Cloud'

Looking ahead to the future, Akers supported rumors that military members will soon be able to 'bring your own device (BYOD)' to work, into a 'Cloud' environment.

The defense science board, a committee of civilian experts appointed to advise the U.S. Department of Defense on scientific and technical matters for the last 50 years, concluded a study looking at Cloud utilization and the security of it.

"The Cloud provides a great level of capability and capacity to solve hard problems quickly and efficiently," said Akers. "Instead of having to build stacks and stacks of computers to solve one hard problem, we can use the Cloud to share all the necessary resources to solve several hard problems simultaneously and quickly."

The technique of 'virtualization' aids the quick problem solving by allowing people to share resources which are otherwise typically underutilized.

There's also a move to stop handing each and every person their own computer. "Instead, they'll get a device like an iPad which will allow them to connect to resources that help them do their job," Akers said. "Through proper implementation of a Cloud, an organization can actually get to a more uniform and resilient security posture."

Akers added, "We can do a better job of patching, setting up security measures and identifying abnormal behaviors due to the formation of the Cloud."

In the same breathe though; he admitted that Clouds bring a special need for protection because they are 'the new big target.' So, he added, "A security of implementations needs to be built in at the onset of a Cloud."

Akers biggest concern remains security. "I worry today about CISCO's products being not just secure enough but unpenetratable to adversary attacks," he stressed. "Adversaries are investing in hacking devices and software more than ever now."

'Hackers – Tactics, Techniques & Procedures'

Akers emphasized, "They (the hackers) are really getting their techniques down pat." Taking advantage of new technologies all the time is important he said because "communities have to be able to operate in an internet environment, but they need infrastructure they can trust."

Adversaries are looking to attack 'the weakest links' such as unpatched workstations, servers, routers and network devices. They also extract important information through direct attacks on individuals or an entire organization.

"No system is impervious," stressed

. . . continued on Page 11

. . . continued from Page 10

Akers. “And you always have to consider your actions online to be susceptible to an attack.” He reiterated many of the warnings that we’ve all heard before.

All employees have to know that: 1) opening unknown or unexpected emails or, 2) clicking on unfamiliar links can create huge opportunities for hackers to commence their operations.

One of the strategies of hackers that he has seen resurge in the past few years has been the use of ‘denial of service’ attacks. A recent example would be when hackers forced a major financial services company offline for several hours.

Financial systems are definitely seeing this sort of hacking at higher rates. “And, classifications of an infrastructure don’t necessarily ensure any extra safety,” said Akers.

A more secure system such as SIPR is in just as much risk as the unclassified network NIPR. “Any infrastructure is susceptible,” he said. “Believing that an infrastructure is secure because of its classification level is one very risky practice.”

In addition to the infrastructure risks, the capabilities of security teams also varies greatly which further increases an organization’s susceptibility to adversaries Akers pointed out.

His advice to Information Dominance Corps Sailors and Officers: “Seriously think about the implications of your actions in particular to the overall security of your entire organization.” Reason why: “Even in the most secure of environments, the human is generally always the weakest link.”

Akers added that “going around any securitypolicy truly creates an opening which can set you up as a target.”

He also provided a warning to gamers. “If you are a gamer, be aware that the adversaries are operating on live sites and will attempt to approach you about how and when you like to play.” Adversaries also try to engage gamers in discussions, appearing just to be another gamer. Spear phishing is based upon human recognizance that helps the adversary know how to craft very high level attacks. “They find out what your hobbies and interesting are by exploitation,” Akers said.

“... going around any security measure truly creates an opening which can set you up as a target.”

Akers told InfoDOMAIN that a company he works with had recently been targeted through a spear phising email that threatened dismissal to any employees who did not ‘click the link’ to update their training records.

“At this point, you have to look at the source of the request, and assess whether you were actually told in any other communications past that the update was going to be expected,” said Akers.

“Rule Number One,” he said. “Distrust an electronic communication until it is verified as secure.” Akers went on to say that the direction we believe we are headed is to an Internet of everything being connected.”

Televisions, refrigerators, coffee pots, entertainment systems, automobiles and several other devices will be, if not already, able to connect to the World Wide Web.

“We have to be able to separate the good from the bad,” said Akers. “It’s important to extract a lot of data from the network regarding what’s going on in the network in order to identify those factors.”

Cellular phone providers already extract information about where people are located and are traveling so that they can target advertising towards the consumer or assist other companies with that information.

Social media sites are doing the same, and they are prime breeding ground for targeting individual users.

“When it comes to personal information, like the type of data that people add to their social media sites, any of it disclosed online is definitely open for attack,” Akers pointed out. “Quite frankly, it’s better to call on the phone to say what you want to say.”

“This pushes us into a big data analysis world in the future,” said Akers. “The only good news is that companies Yahoo and Google have both begun encrypting emails while they are in transit.”

“Watch floor and cyber employees should definitely be using one of the two carriers,” he suggested. “It assures that someone can’t watch traffic on the wire and pull it out and read it.”

Akers still feels that financial institutions and banks tend to be more trustworthy places, at least large name banks which are known to be investing heavily in security. “But sites that exchange money or do payment clearing houses - watch out,” he said. “Always look at the top of the web browser on that site URL to ensure that encryption is being used.”

‘Protecting Yourself, Protecting the Mission’

His candid advice to all Sailors – “Protect yourselves while online. Don’t EVER mix mission information with personal activity.” Akers confirmed that Sailors and other military members literally do get spear phished, and he emphasized that an adversary can use your information to attack a shipboard mission.

“We’ve already seen such adversarial tactics, techniques and procedures in play worldwide,” said Akers. “Missions can be compromised by the adversary simply denying, deceiving, destroying, or discovering mission critical information.” He went on to say that “systems can be so infiltrated that they can never be trusted for use again.”

“The devastation can literally cost millions of dollars, or even worse, a failure of mission that can cost lives,” said Akers. “Just imagine a blue force tracker that isn’t trustworthy.....and troops might literally not be located during a dire moment.”

Akers concluded his interview with a key point: “You can’t deny the possibility of you yourself becoming a target because statistics show that it’s very probable.”

“The bottom line,” he stressed, “is that any attack on any government or military person that is successful can and will possibly result in a mission failure that might even involve the loss of life.”

Martial arts Mirrors Military Life - Navy Comes out on Top

By CTI2 (IDW) Deejin Macaraeg, CID Public Affairs

MONTEREY, CA – The reigning Women's World Martial Arts Champion is bringing her championship drive and spirit to her studies at the Center for Information Dominance (CID) Unit Monterey.

ET3 Sonie Lasker, a student assigned to the CID Unit Monterey and attending the Defense Language Institute Foreign Language Center (DLIFLC) to learn the Persian language known as Farsi, is not only excelling at her studies, she is sharing her knowledge, discipline and experience of the martial arts to fellow service members on and off the mat.

Before joining the Navy in 2010, Lasker was the team captain of the United States Martial Arts Team. She competed in more than 500 tournaments worldwide and was a 14-time world champion.

At the end of the 2010 World Martial Arts Games, Lasker was standing on the podium receiving another gold medal. As the national anthem played, she was overwhelmed with emotion and gratitude to the United States for having the freedoms that allowed her to achieve so much.

After so many years of having the freedom to compete, and the honor to represent the United States in world competition, Lasker felt this overwhelming compulsion to give something back to her country that had given her so much.

In that moment, at the age of 38, she decided to join the Navy.

As an older student, Lasker explained how the life of a martial artist is similar to military life and what made her choose the Navy as the branch of service she would serve in.

"Martial arts and life in the military go hand-in-hand," Lasker said. "Martial arts are of high moral character and focus on the same core values as the Navy; honor, courage and commitment."

Since arriving at DLIFLC, Lasker has taught Brazilian Jiu-Jitsu, Judo, and grappling to service members from the Air Force, Army, Navy and Marine Corps five days a week at the Price Fitness Center on the Presidio of Monterey. In addition, after only two weeks in class, her teaching staff recognized her as a 1+ student in speaking the foreign language she is attending at DLIFLC.

A (1+) in speaking characterizes use of a spoken language. On a scale from zero to five, each higher level implies control of the previous levels' functions and accuracy.

Lasker maintains a 4.0 grade point average in her foreign language

. . . continued on Page 13

. . . continued from Page 12

class and spends time on weekends tutoring other students, which she was encouraged to do by her teachers.

Lasker continually strives to help build unit cohesiveness and supports the morale of her fellow service members.

"The responses that I've been receiving from the students here at DLIFLC, who come to my sessions [martial arts and tutoring], have been very humbling," Lasker said.

"I'm extremely appreciative of Petty Officer Lasker taking the time to help me understand how to read Farsi," Seaman Adrienne Weaver said.

"The tools that she has provided me during our Jiu-Jitsu training sessions is something I will take with me and use in my everyday life," Lance Cpl. Elvis Costa said.

As a black belt and national certified trainer in martial arts, Lasker has the authority to rank her students to the level of white belt. Since her training sessions began in 2012, she has ranked eight service members.

In August 2012, Lasker heard about the 2012 U.S. Open Brazilian Jiu-Jitsu Tournament taking place at Independence High School in San Jose, Calif. She started training her students for the competition.

After only two months, the team, called the Joint Service Martial Arts Machado Fight Team, was ready for the competition on Oct. 6.

There were more than 800 competitors and each match lasted about five minutes. There were broken lips, bleeding, and dislocated joints within the first hour.

"There were a lot of injuries going on that I saw," Lasker said. "Luckily, the way that we train is to avoid major injuries. One of our competitors had a split lip, but that was the extent of it."

Every competition was intense and every white-belt gave it his/her all. They attempted to apply joint-locks, chokeholds, and pull guard as well as mount their opponents or throw them on their backs. All of the competitors from DLIFLC competed for more than six hours.

After the students were done competing, Lasker congratulated her students.

"I am so proud of them," she said. "They worked so hard, were respectful, remained combative and showed their training. They did a great job."

63 YEARS LATER, KIDS ARE STILL LEARNING FROM SAILORS

From CID LS San Diego Public Affairs

SAN DIEGO – Sailors assigned to Center for Information Dominance (CID) Learning Site San Diego recently visited the Arroyo Vista Elementary School to volunteer as part of the Junior Achievement Program.

"Community relations projects are an important tool for the U.S. Navy to give back to the communities we live in," CID LS San Diego Director LTJG James Whitman said. "The partnership we have with the Arroyo School is a wonderful opportunity for our Sailors to volunteer their time."

CID LS San Diego's mission is "To deliver full spectrum Cyber Information Warfare, and Intelligence Training to achieve decision superiority." In addition to their military duties, CID LS San Diego provides mentors, tutors and role models for various organizations throughout San Diego County.

"The teachers were very impressed by the Navy volunteers and truly enjoyed having them," Education Manager Valerie Hash said. "I cannot wait to host another Junior Achievement Day with Navy volunteers."

"The children were well behaved," CTR1 Nicole Duran said. "It was nice to hear a couple of the students say that their parents wore the same uniform."

"The children were very knowledgeable about the Navy," CTTCS Mayra Kohlmann said. "There was a student who told me their parent was a pilot and another said theirs was a doctor on a ship."

Sailors who participated in the event said they enjoyed the opportunity to interact with the children and bring the Navy to the school.

Junior Achievement of San Diego and Imperial Counties has been serving area students since 1950.

Junior Achievement is a worldwide nonprofit founded in 1919. They provide work force readiness, financial literacy, and entrepreneurship curriculum and training to students from kindergarten through twelfth grade.

Their goal is to prepare young people to enter the real world with applicable skills and knowledge that will better prepare them for jobs, higher education, and future business opportunities as productive citizens in a global economy.

EDITOR'S NOTE: ***CID is the Navy's learning center that leads, manages and delivers Navy and joint force training in information operations, information warfare, information technology, cryptology and intelligence.***

IT1 Nicole Duran, the midgrade CID Domain Instructor of the Year, spends time with a student at Arroyo Vista Elementary School. Duran, along with fellow CID Learning Site San Diego instructors, volunteered at the school as part of the Junior Achievement (JA) Program. (Official U.S. Navy photo)

FIVE DAYS TO FINE TUNE THE FIVE C'S

SHIPBOARD C5ISR PUT TO THE TEST

Story & Photos by MCSN Hunter Harwell

Challenge:

A Carrier Strike Group or Amphibious Ready Group along with its Marine Expeditionary Unit (CSG/ARG/MEU) is preparing to deploy, and the ships' systems aren't operating at 100 percent capacity on board or in conjunction with the other ships in the CSG/ARG. Having all C5ISR (Command, Control, Communications, Computers, Combat Systems and Intelligence, Surveillance and Reconnaissance) fully interoperable is imperative to the success of any deployment.

Solution:

This is when a team of subject matter experts (SMEs), conducting robust and thorough systems interoperability validation checks during Composite Unit Exercise (COMPTUEX) is needed to get the ships' C5ISR systems in tip-top shape before deployment. A successful COMPTUEX is required of each group of ships before they are authorized to deploy.

A team of SMEs get just five days and four nights to solve all the issues and bugs that the many C5ISR shipboard systems might present. With only five days to test ships' systems, and to train and mentor Sailors and Marines operating those systems (some for the first time), members of the elite Deploying Group Systems Integration Testing (DGSIT) team will be needed to stay on point, day and night, during the exercise, remaining motivated and tenacious, or the ships might not complete COMPTUEX and be authorized to sail in the Spring.

Navy Cyber Forces, the executing organization for all Fleet DGSIT operations, typically sends up to 60 of the finest and most talented civilians and military personnel, all SMEs on one or more systems, to test, fix, train, mentor and, if needed, recommend work-arounds for the harder fixes during COMPTUEX - a 'fully stressed' operational environment for both the crew and systems. Such conditions have historically proven to be the most productive time for the DGSIT's Final Integration Testing to ferret out outstanding issues before the CSG/ARG's big day - deployment.

Each of the DGSIT team members, viewed as experts in their respective field, have much to accomplish upon arrival to their assigned ship with no time to waste. DGSIT SMEs do not deploy, so training and mentoring of Sailors and Marines is one of the most important bi-products for the team during testing.

Sailors of USS Kearsarge (LHD-3), the largest ship in the ARG, along with its Marines from the 26th MEU, participating in COMPTUEX off the east coast of the United States, are being assisted by the DGSIT SMEs. They are conducting the COMPTUEX along with

. . . continued on Page 16

. . . continued from Page 15

USS San Antonio (CG- 56) and USS Carter Hall (LSD-50). The three ships comprise the Kearsarge Amphibious Ready Group (KSG ARG).

A novice sitting in the DGSIT's briefings would drown in the sea of acronyms of odd systems names: GEEKS; DOTS; JUMPS. Twice a day, SMEs update the systems they're working on, clarifying difficulties, improvements and goals to be reached over the five days shipboard. Also briefed is the progress made mentoring Sailors and Marines.

"It's a real synergy, the bringing together of multiple SMEs with the ship's crew during a stressed operational environment," said Randy Fenz, a DGSIT team lead. "Talking and collaborating between the SMEs and ship's crew is sort of like an arranged marriage - people work together for better or for worse."

"This is the final integrated testing for pre-deployment," said Staff Sergeant Dana Margulies, a Marine and a DGSIT SME. "These guys are getting ready to punch out of here," said Margulies. "So, we're here aboard the ship to make sure everything is in its place and is set up the way it's going to be once they get underway."

When Marines first attend computer school, they are taught basics – how to use a computer, how to assign an IP address, and, how to make routers talk to one another. "There are a lot of things they are not taught in the school house," said Margulies. "The DGSIT team assists with that additional training."

He added, "Once the ship gets underway, we won't be there to help. Our goal is to prepare them as best we can." Still, Margulies explained that the MEU Marines can continue to receive technical support while deployed by phone or by email.

Margulies is the Marine Corps networks and Host Based Security System (HBSS) SME, a system on the green, or unclassified, side. He recognizes several challenges that the MEU is facing during the five-day evolution with the DGSIT. "Everybody is stretched very thin," Margulies noted. "We have Marines wearing many hats and spending their time working different things."

Margulies found it extremely difficult just to get a solid two-hour block with Marines he was mentoring in order to show them the systems without them getting pulled for other collateral duties. The majority of the MEU Marines come from the Communications Battalion,

. . . continued on Page 17

. . . continued from Page 16

8th Marines at Camp Lejeune, NC, and they are formed up a year prior to the deployment to begin training and conducting work-ups.

Training and mentoring time spent with the DGSIT SMEs is imperative since some of the systems' problems don't even present themselves until the SMEs are working alongside the Sailors and Marines aboard ship. The process proves to be a real challenge with the ship's company and MEU Marines already training and providing for the COMPTUEX between the three ships of the KSG ARG.

During the at-sea exercise, all newly fielded, recently installed and upgraded systems are fully evaluated. SMEs spend the majority of their time with ship's crew. Together they fully employ all the systems, attempting to uncover problems, identify systems limitations, and then, coordinate the best resolutions or assist with potential work-around options to problems not immediately resolvable.

Bottom line - There's a ton of knowledge the team must impart, the success of which builds on what Sailors and Marines already know.

The SMEs embark all of the ships, conducting more than 300 types of evaluations, which typically uncover many C5ISR systems issues. "Each SME support specific shipboard missions and systems," said Margulies. "But, if we have information on something else, then we can provide training on that system as well." As a result, most problems are corrected before the SMEs departure.

So, can these DGSIT SMEs be considered Fleet Super Heroes? The SMEs might say 'No.' They would all admit, however, that they are a passionate group, most of whom, but not all, are prior Sailors or Marines. Several spent years aboard ships. Others are civilians recruited specifically for their breadth of systems knowledge, both old and new, and for their abilities to resolve C5ISR problems that could hinder a ship's performance at critical moments.

The SMEs closely observe the challenges Sailors and Marines encounter with the systems, and offer thousands of mentoring man-hours.

. . . continued on Page 18

. . . continued from Page 17

For those who have been a part of the DGSIT team for several ships' visits, they're often employ past work-arounds on systems, saving less-experienced military members significant time and aggravation.

Richard Billings, a long-term DGSIT team member and retired Navy Chief said he unexpectedly found himself as an Automated Data Processing Officer on board his last ship. "It was like drinking from a fire hose," said Billings, when it came to understanding the job. Before the IT rating ever existed, Billings was assigned the job simply because he was 'into computers.' "Shipboard networks back then were sort of like the Wild Wild West," Billings recalled. "There was no standardization at that point."

Eventually the Navy finalized "IT21" – Information Technology for the 21st Century, which standardized shipboard network systems.

Before leaving active duty in 2001, Billings said he actually remembers a DGSIT team coming aboard his cruiser. "Our system was working well at the time because it was brand new," he said. "Still, they helped out with understanding a few things."

Billings first served as a DGSIT member aboard USS George Washington (CVN-73). Several years since his first experience, he understands pre-deployment challenges some ships face, especially if the ship spends extra time in the shipyard beforehand, as in Kearsarge's case.

"Even though I've been an IT for almost eight years," said IT1 Christopher Pulley, who worked closely with Billings aboard Kearsarge, "he (Billings) will come in and draw a picture on the whiteboard and explain 'this is why we do things this way.'" Pulley emphasized how it 'made troubleshooting problems ten times easier' for his Automated Data Processing group.

The relationship the DGSIT SME and the Sailor or Marine first establish is an important one. "You don't realize until you get to the ship and get hands-on experience, and then something breaks, how much more intensive the job is," said Pulley. Working with a problem firsthand, and under the guidance of the DGSIT SME, Sailors and

. . . continued on Page 19

. . . continued from Page 18

Marines get a close up look at what they need to fix systems problems.

"No matter how big, I can now troubleshoot all problems," said Pulley, after spending the five critical days with his mentor Billings. "The main goal is for us, the techs, to be self sufficient."

It's vital that Pulley and others get ample time to utilize the SMEs past experiences and mentoring time to learn during COMPTUEX. "It gives me a sense of comfort that someone I now know, who knows what he's doing, has looked over my system and said that we are ready to go on deployment."

Even with these 'Fleet Super Heroes' working around the clock, complex issues requiring a significant level of repair, are left open for resolution before the ship's next deployment. Everything down to a CSG's or ARG's capability to communicate with coalition ships is considered so ships are ready to work with allied forces at sea.

Before the visit is concluded, DGSIT team leaders prepare an in-depth brief for the CSG/ARG Commander and key staff members, outlining systems issues discovered, the follow up required for resolution, as well as the level of mentoring and training conducted with Sailors and Marines.

"Systems today are so much more complex than years ago," said DGSIT Event Director Owen Kink, who's involved with most of the CSG/ARG five day evolutions. "Knowing how the systems interface together, working around the types of problems you can encounter with them," said Kink, "are all tools that we, as mentors, have to do our best to pass along to Sailors and Marines."

At the end of the five-day stint in which the whole team had worked so tirelessly aboard the KSG ARG, Kink and his other team leads Randy Fenz, Paul Minner and Daryl Davis all heard the feedback they'd been waiting for from ARG Commodore Brad Skillman. "The amount of work that was accomplished by the DGSIT team in such a short period of time is very impressive and shows how vital this team is to the success of each deployment."

Even though the ARG's ships turned a major corner in preparation for deployment, extra care of the C5ISR systems would still be needed according to the management team's final comprehensive brief.

"Each of the ships of the ARG are of different ship classes and have different configurations for their communications, and, command and control equipment," Skillman explained. "Although two of our three ships communicated well during our last deployment, upgrades to individual systems may not be synchronized between them."

For amphibious ships, Skillman pointed out that there is an added complexity with many Marine systems riding on Navy network backbones. "DGSIT is designed to solve these problems," he said. "They bring experts who not only help the operators and the equipment perform well, they also ensure that the equipment can work as it was intended between the various ships and commands. Invaluable support!"

He further emphasized how important it was for the KSG ARG to have been given such an 'honest and fair evaluation.'

After countless hours on the systems, mentoring and training Sailor and Marines, and evaluating and solving a plethora of problems, the SMEs managed to squeeze in half of a good night's sleep their last night aboard the ships. When the DGSIT management team concluded their brief, the Commodore left them with a parting assessment of the process.

"For you to come out with us only a month away from deployment, and for the ARG to check out 'OK,' leaves me with a great deal of confidence," said Skillman. "Your findings, along with the training you gave to our crews, will make us that much more effective for deployment and beyond."

Additional content and photos from CDR Brenda Steele MacCrimmon

STEM Gets Thumbs Up from CYBERFOR

The Honorable Kenneth I. Wright, Portsmouth's Mayor, introduces RDML Gretchen S. Herbert, commander, Navy Cyber Forces, during a Science, Technology, Engineering and Mathematics (STEM) program at Woodrow Wilson High School.

Story & Photos by MC3 (SW) Jacob D. Galito

PORTSMOUTH, VA -- RDML Gretchen S. Herbert, commander of Navy Cyber Forces, and the Honorable Kenneth I. Wright, mayor of Portsmouth, spoke to elementary through high school students and their families during a Science, Technology, Engineering and Mathematics (STEM) exhibition at Woodrow Wilson High School, Portsmouth, VA. Navy Cyber Forces, Naval Network Warfare Command and Navy Cyber Defense Operations Command teamed up to to students and family members about their technical career paths in the Navy during the one-day exhibition.

Any young person choosing a STEM field will find jobs are wide-open into the future when they graduate high school & go to college.

The STEM event is conducted annually in an effort to promote interest in the four primary technical fields amongst both male and female youth ranging from elementary to high school.

STEM Outreach Coordinator and Navy Cyber Forces Diversity Director Sandra Anderson pointed out that while "one-third of all eighth-graders are interested in technical degrees for college, by the time they are seniors in high school, only six out of 100 want to pursue a four-year degree in a STEM field."

Anderson therefore emphasized the importance of such events like the Portsmouth STEM Day which exposes the area school students to young adults like Cyber Forces Sailors who currently serve in such fields. "The Sailors are able to spend time one-on-one with students who express interest in one of the STEM fields," said Anderson.

Over the next 5 years, the Navy is investing millions of dollars into STEM educational programs for students.

8 out of 10 college degrees in computer science, engineering and physics were earned by men. Only 1 in 7 engineers were females, and only 27% of computer science workers were.

(Left to Right) CTNC Kristi Windham and CTNC Tamika Cobb, assigned to Navy Cyber Defense Operations Command (NCDOC), speak to a student during a Science, Technology, Engineering and Mathematics (STEM) program at Woodrow Wilson High School. NCDOC, Navy Cyber Forces and Naval Network Warfare Command participated in the STEM program in support of students persuing education within the STEM fields.

Virtual Training Honors Award

By LT Scott Cunningham, FITC Public Affairs

SAN DIEGO– A Fleet Intelligence Training Center (FITC) civilian was awarded the 2013 Copernicus Award during the Armed Forces Communications and Electronics Association (AFCEA) national conference in San Diego, January 29-31.

The AFCEA met to discuss advances in their field and honor those who have made particular strides in innovation Among the conference honorees was Frank Watson, department head for the Systems department within the Fleet Intelligence Training Center (FITC).

Responsible for all operations, acquisition, installation, integration, and maintenance of Technical Training Equipment (TTE) at FITC, Watson was recognized for his hard work by being awarded the 2013 Copernicus Award.

AFCEA is dedicated to increasing knowledge through the exploration of issues relevant to its members in information technology, communications, and electronics for the defense, homeland security and intelligence communities.

In fulfilling that mission, AFCEA and the U.S. Naval Institute (USNI) established the Copernicus Award in 1997 to recognize individuals, based on their sustained superior performance and contributions, to naval warfare in Command, Control, Communications, Computers and Intelligence (C4I), information systems, and information warfare.

Nominees must have made specific, demonstrable contributions of a technical nature which should involve exceptional initiative, leadership and insight within the nominee's area of expertise. All Navy, Marine Corps, Coast Guard, personnel (including joint/NATO) commands, afloat and ashore and civil service were eligible for nomination.

The selections are made each year by Navy judges who review applications from the Navy, Marine Corps and Coast Guard, including active duty and civilians.

It was Watson's work on and implementation of a Virtual Desktop Environment (VDE) which secured him the national recognition.

In addition, VDE implementation at FITC initiated a larger effort to update the training network structure across the entire Naval Education and Training Command domain.

VDE is envisioned to enable forward-based training elements, ashore and afloat, to access training applications hosted at a single location and remains one of the best options to improve fleet training while realizing numerous cost efficiencies.

Extending VDE implementation could be one of the best possibilities moving forward to upgrade school house systems while taking advantage of the decreased manpower used to keep the system up and working.

"Mr. Watson's efforts in leading the virtualization push from FITC made him a great candidate for the Copernicus recognition," FITC Executive Officer Lt. Cmdr. Lance Taylor said. "I am glad the AFCEA community wanted to recognize him for his work."

For more information on the Fleet Intelligence Training Center, visit the FITC information page on CANTRAC or through NETC: https://app.prod.cetars.training.navy.mil/cantrac/pages/rpt_vol1.html?uic=43662 https://www.netc.navy.mil/centers/ceninfodom/fitc/CommandInfo.aspx?ID=0

CID is the Navy's Learning Center that leads, manages and delivers Navy and Joint Force training in information operations, information warfare, information technology, cryptology and intelligence.

CIO's Network Tips

HOUSE CLEANING RULES FOR YOUR CYBERWORLD

By Carlos Parter, Fleet Cyber Command

The year was 1995. The family was growing and it was time to set up a new homestead. We searched and searched and finally found a big house with a large yard to accommodate our growing family. The house came with a two car garage, large attic and four bedrooms. The new house seemed so empty after we moved in. It was nice having both cars in the garage and all the extra space in our new home.

Fast forward to today; the large house doesn't seem large anymore. We have not been able to park the cars in the garage for years. It appears, overnight, we acquired a mountain of stuff. Now, the storage shed, attic and garage are bursting at the seams with boxes of documents we have not opened in years. To add to the misery, the storage rental unit we've had to acquire will cost a bundle each month. How did we get to this stage? We are in dire need of a records management system equivalent to evaluate what we need to keep and what we need to get rid of. We cannot afford to buy a bigger house or continue renting a storage unit. Many of our neighbors find themselves in the same predicament.

Somebody save us!

Why Records Management?

According to a 2008 U.S. Department of the Interior article, every business or program must address well-defined objectives that add value, either directly to the bottom line or indirectly toward the achievement of the organization's goals and objectives.

Record Management (RM) programs must manage organizational information so it is timely, accurate, complete, cost-effective, accessible and useable. Better information, at the right time, results in better operational decisions and makes good business sense.

Following are some important reasons to set up a good records management program:

- To control the creation and growth of records
- To reduce operating costs
- To improve efficiency and productivity
- To assimilate new records management technologies
- To ensure regulatory compliance
- To minimize litigation risks
- To safeguard vital information
- To support better management decision making
- To preserve corporate memory
- To foster professionalism in running the business

Department of Navy (DON) records are documentary materials, regardless of physical form or characteristics, made or received by a DON command, activity, or office (DON organizations) that provide evidence of an organization's structure, functions, policies, procedures, decisions, operations, and other activities.

DON organizations are also required by statute, federal regulations, and directives to manage records in accordance with prescribed procedures and processes. These policies are enforced in the Navy Records Management Program, OPNAVINST 5210.20.

The Navy assigns disposition and lifecycle of records through the Standard Subject Identification Codes (SSIC). An SSIC is a code that is assigned to determine the periodicity of a record. SSICs range from the authority to delete files after three months (e.g., general e-mail correspondence) to the requirement to keep the records permanently (e.g., command policy decisions). In fact, DON has over 7500 SSICs that categorize all types of records created. This information can be found in the DON Records Management Manual, SECNAV M-5210.1. Legally, a Navy record is not authorized for destruction unless it has exceeded its SSIC periodicity.

The following are the benefits of a

"Network man says efficient records management helps our shared network run like a well-oiled engine."

sound RM program that allow personnel to be more productive employees:

- Provides efficiency in locating records in a timely manner
- Ensures the most current file is being produced and satisfy Electronic Discovery (eDiscovery) requirements (eDiscovery includes word documents, spreadsheets, emails, audio and video files, etc.)
- Maintains legal compliance. Personal Identifiable Information (PII) and privacy act information can easily be identified and protected to satisfy eDiscovery requirements
- Preserves Historical Legacy Records that are managed and maintained to effectively tell the story of the command's existence

See list below as a reference of what may constitute a record:

The Navy/Marine Corps Intranet (NMCI) offers a Records Management

. . . continued on Page 23

. . . continued from Page 22

Is It a Record or Not?	
Records documenting any Navy mission-related activities (Program Records)	Yes
Records documenting routine Navy housekeeping support activities (Administrative Records)	Yes
Any transactions related to agency business	Yes
E-mail	Yes; except personal content
Active "working files" that document work being done by an Action Officer	Yes; but, working copies may often be destroyed after final document is published
Documents not connected to transactions of agency business (personal files)	No
Extra copies of documents, stocks of publications, library and museum material	No

Application (RMA). RMA is Electronic Records Management Software Applications Design Criteria Standard, DoD 5015.2 compliant, Functional Area Manager (FAM) approved, and Freedom of Information Act (FOIA) certified. Total Records and Information Management (TRIM) is deployed to every seat on NMCI, both NIPRnet and SIPRnet, and is a NMCI core build content. TRIM is the only approved electronic system for storing official Navy records. Our deployment of TRIM is compliant with SECNAV instruction M-5210.1, to allow records lifecycle to be managed by SSIC. In addition to RM, TRIM offers a robust searching tool with over 100 built in searches and the ability to search for command specific metadata.

TRIM will always display the most recent version; however, all prior versions remain accessible in the properties section of the record. Displaying the most recent version ensures the file produced in a search is the latest and the ability to retrieve prior versions are easily achieved. TRIM has a highly customizable workflow feature, tight integration with Outlook, and a redaction tool.

For NMCI users, below is a list of additional official file locations:

- Share drive- Collaborative working environment for short term usage; not intended for storage (less than one year).
- The command File Share is used to post official information for personnel to view and use
- End users are granted necessary permissions to access folder content in the NMCI file share environment
- End users may perform their work by sharing official files with a work group or to obtain information from the file share
- The end user is responsible for clean up/purge of files no longer required. Completed project work files with informational value should be moved to TRIM. Files that are out-of-date or have not been accessed for over a year should be archived into a backup repository
- The command file share is not a repository for archived files
- Shared space will not be used for unofficial data or files, as it would deprive the command of space for official data
- Unsuitable files include: Personal .pst files, unofficial multi-media files, executable files (.exe)
- Portal - Collaborative working environment for short term usage; not intended for storage
- Home drive – can be used to store any critical, work-related data or e-mail for routine backup
- See Navy Telecommunications Directive (NTD) 10-11, OPNAV FORM 5239-14 (REV 9 2011), System Authorization Access Request Navy (SAAR-N) for additional guidance

An office with files scattered and stacked on top of file cabinets and in boxes, creates an inefficient working environment. The same applies to electronic records. One of the key issues caused by improper RM, relates to cost.

For example, the available storage space shrinks and command history files could be inadvertently deleted or hard to find. Acquiring additional storage space is a temporary solution that eventually becomes cost prohibitive. Dependent on the number of users, a command may require anywhere from 100 gigabytes to a terabyte of share drive space.

The image and morale of a team relies on productivity is among the best reasons to maintain a good RM program. Moreover, in a time of budget restraints and demand for efficiency, we must have an active and effective RM program in place.

What can each of us do to help? It all comes down to doing periodic house cleaning. Delete old files, especially draft and other working documents. Remove outdated files from portals, web sites, share drives, or personal drives. Make it a habit.

References and Resources:

US Department of the Interior Records

Management Questions:

SECNAVINST M-5210.1, January 2012
SECNAVINST 5210.8D, 31 December 2005
OPNAVINST 5210.20, 21 December 2010
Department of Defense 5015.2, 25 April 2007
Navy Telecomm Directive 10-11.

"Stay safe my friends & remember efficiency equals savings!"

Task Force Urgent Sentinel

Fleet ballistic missile submarine, USS Alaska (SSBN 732) arrives at Naval Submarine Base Kings Bay, GA. The Alaska, increases the number of fleet ballistic missile submarines at Kings Bay to six. (Photo by MC1 Kimberly Clifford)

By MC1(IDW/SW/AW) Elizabeth Burke, NETWARCOM Staff Journalist

Emergency Action Messages (EAMs) are highly structured, authenticated messages used in the command and control of nuclear forces. Nuclear-powered ballistic missile submarines, the most resilient leg of the nuclear triad, carry submarine-launched ballistic missiles that can only be launched by Presidential order directed through EAMs.

In May of last year, the Navy identified a series of anomalies that affected the confidence in our ability to successfully execute the U.S. Nuclear Command, Control (NC2) mission. Fleet Cyber Command (FLTCYBERCOM) directed the stand-up of Task Force Urgent Sentinel (TFUS) to conduct a thorough review of the entire process, relating specifically to EAM delivery, and recommend improvements to ensure 100 percent continuity of communications.

A wave of issues occurred in winter 2012 that brought this issue to a head. "Anything that impacted the ability to deliver an EAM was significant and considered an incident or an outage," said Michael Jones, Enterprise Management Division Director. "This was the first time there was a dedicated, resourced effort to resolve our shortfalls and more detailed analysis determined that these incidents had been occurring over several years."

NETWARCOM's TFUS support stood up in April 2012, to identify the root cause of the lapses in NC2 connectivity with a five member team from Commander, Naval Network Warfare Command (NETWARCOM)/Commander, Task Force 1010 (CTF 1010). The team was selected for the previous Navy experience of its members and focused in two primary areas: messaging and Very Low Frequency(VLF)/Low Frequency(LF) communications. The team members included Terry Robinson, team lead, Edward Crumb and John Halmrast, VLF/LF communications and Virginia Lundy and Randy Sorenson, messaging.

The team first established a baseline for analysis, building a database from scratch. Months of data was collected from more than 50 sites worldwide on outages ranging from equipment to hardware, software, maintenance and Standard Operating Procedures (SOP) issues. They tracked more than 600 events.

Once trends were identified, the team worked with Space and Naval Warfare Systems Command (SPAWAR) to develop solutions.

"When we found that something kept repeating itself or if something was really catastrophic then we would send that information to SPAWAR," said Halmrast. "SPAWAR has the engineers and the know how to really dig deep to resolve the issues."

Once they started to probe the problem areas, more issues were discovered.

"Some of those problems you wouldn't see unless we were looking," said Crumb.

"So when we started looking real hard we found that things happened more than they should, but wouldn't have been identified if TFUS hadn't been established."

"The system that routes these messages is designed so that if a site goes down another site will pick it up without missing a beat," said Halmrast.

"As soon as a circuit drops out it's routed to an alternate site so you are not noticing that an outage ever occurred," said Robinson.

The team's recommendations were submitted to the TFUS Executive Steering Committee, along with inputs from NETWARCOM and SPAWAR. Funding was obtained by OPNAV N2/N6 to implement the improvements that were identified.

Over the last year, TFUS has seen a decline in the amount of events reported. This is directly attributed to the suggested improvements that NETWARCOM and SPAWAR implemented.

In January 2013, the NETWARCOM TFUS team was recognized with a Special Act award by NETWARCOM Commander, CAPT John W. Chandler, for its actions in support of EAM delivery.

A FEW SAILORS HONOR MANY VETERANS AT WWII MEMORIAL

Official U.S. Navy Photo

By YN2(AW) Ramos

Joint Base Andrews' service members greeted veterans from across the United States at the World War II Memorial on Saturday, April 21.

More than 400 veterans shared their knowledge of military heritage, history, and etiquette they experienced with current active duty service members during one of many events held in the Washington, DC, National Mall.

Five active duty Sailors, of different ranks, from Naval Communications Security Material System volunteered at the "World War II Veterans Meet and Greet" event. Amongst the five Sailors, Petty Officer First Class Marquise Hodges stated, "I really enjoyed hearing the stories from actual people who were involved in World War II. It was time well spent spending time with those who paved the way for our current military."

The World War II Memorial opened to the public on April 29, 2004. Veterans begin to start gatherings at the memorial starting in April and ending in September each year.

The Culture of Responsible Choices (CoRC) sponsored the event to meet and greet the veterans. CoRC is a program on Joint Base Andrews that sponsors volunteer opportunities for military members and promotes responsible behaviors through leadership, individual, base, and community-level involvement -- underscoring responsible behaviors.

NIOD JACKSONVILLE

1ST COMMAND TO QUALIFY EIDWS

On Dec. 13, 2012, Navy Information Operations Detachment (NIOD) Jacksonville, formerly Naval Security Group Detachment (NSGD)Brunswick, Maine, was recognized for becoming the first command in the Navy to qualify for the Enlisted Information Dominance Warfare Specialist (EIDWS) Pennant for having attainted 100% of its enlisted personnel qualified as EIDWS specialists.

NIOD Jacksonville provides Information Warfare and cryptologic direct support to CNO-sponsored Airborne Special Projects and is an Echelon V command subordinate to Navy Information Operations Command (NIOC) Georgia. All Sailors from Jacksonville are hand-selected from the Navy's finest Naval Aircrewmen to execute national and theater-level tasking around the globe.

In a ceremony onboard Naval Air Station Jacksonville, FCC/TENTH FLEET Command Master Chief (CMC) Christopher Welch presented the EIDWS pennant to NIOD Jacksonville's OIC, LT Jamie Davis; Senior Enlisted Advisor, CTRC(IDW/NAC/AW) Shane Gammon; and the Detachment EIDWS coordinators, CTI1(Ret) Michelle Kwon and CTI1 (IDW/NAC/AW) Joshua Weaver. Also present to witness this historic milestone were CAPT James Brokaw, commanding officer, NIOC Georgia; CDR Todd Gagnon, NIOC Georgia's XO and NIOC Georgia's CMC Larry Howard.

In accordance with Navy policy, NIOD Jacksonville is authorized to fly the pennant for 12 months from the date of award. Due to its Dec. 31, 2012 decommissioning, the pennant was flown at the Detachment until its closure, after which time it is presently being displayed at NIOC Georgia. The awarding of the EIDWS pennant signifies yet another significant accomplishment for this storied Detachment, even as it prepared to close its doors after nearly four decades of exemplary service and operational excellence. Since the Detachment's decommissioning, the legacy of NIOD Jacksonville/NSGD Brunswick continues to endure.

(Left to right) CAPT James Brokaw, LT Jamie Davis, CTI1(ret) Michelle Kwon, CTI1 Joshua Weaver and CMC Christopher Welch. (Photo by LTJG Kevin Wendt)

BOLD ALLIGATOR '13

. . . PREPAIRING FOR DISASTERS

By LCDR Weylin Piegorsch, NR NCTAMS LANT

The U.S. Navy has a proud legacy of service. It has earned its place as the premier Navy in the world, and one of the best in all of history. But the Navy still has many opportunities for improvement.

The area of Humanitarian Assistance and Disaster Relief (HA/DR) allows the Navy to use its impressive capabilities to support its role as a 'Global Force for Good'. Unfortunately, opportunities to participate in HA/DR are situational-dependent and lessons previously learned need to be re-learned; like how to interact with foreign- and non-government organizations (FGO/NGO) and how to interact with a civilian population.

". . . Humanitarian Assistance and Disaster Relief allows the Navy to support its role as a 'Global Force for Good'."

Thankfully, there are several organizations within the Navy working to bolster this area. When CAPT Danelle Barrett assumed command of Naval Computer and Telecommunications Area Master Station – Atlantic (NCTAMS LANT) in late 2011, she set the affiliated Reserve unit to the task of studying planning in the areas of communications and knowledge management.

This past April, the Reserve unit put its new-found skills to the test by supporting Expeditionary Strike Group TWO (ESG-2) during operation Bold Alligator2013 - a multi-national exercise focusing on regional incident response, culminating in an HA/DR scenario.

CDR Blake Eikenberry, ESG2 N6, had high praise for the support from NCTAMS LANT in general, and of the

. . . continued on Page 27

Illustration by MC3(SW) Jacob D. Galito, CYBERFOR Public Affairs

. . . continued from Page 26

(Clockwise) ITC Scott Schindler repairs some wiring. ITC Derrick Owens and IT1 Robert Jenkins review equipment configuration settings in support of operation Bold Alligator '13. ITC Owens and Marine MSgt. Jermalia Turpin double-check their settings. MSgt. Turpin and ITC Schindler discuss operational aspects of operation Bold Alligator '13. (Official U.S. Navy Photos)

Reserve unit specifically. "NCTAMS LANT Reservists were instrumental in advancing our readiness for the exercise," said Eikenberry. "In addition to basic preparations such a equipment setup, they also supported Information Assurance preparations and provided knowledge management support for the event's Collaboration At Sea (CAS) and Combined Enterprise Regional Information Exchange (CENTRIXS) systems."

This support continued throughout the entire event. Responding to numerous technological issues, NCTAMS LANT Reservists provided continuity of operations. Between troubleshooting failed equipment, correcting account configurations, and training exercise participants on system use (particularly important for the foreign military personnel participating in the exercise), Reserve personnel acquitted themselves well.

"This entire team had no trouble integrating into ours and was a big value added for executing BOLD ALLIGATOR '13," said Eikenberry. "I sincerely appreciate the assistance rendered and the camaraderie gained."

". . . Humanitarian Assistance and Disaster Relief allows the Navy to support its role as a 'Global Force for Good'."

Flags Flown at Half-Staff; Arizona Honors Fallen Sailor

CTTC(SW) Christian Michael Pike died from injuries suffered in Afghanistan March 10. (Photo courtesy Naval Special Warfare Command)

From Independent News Media, Inc., USA PHOENIX

Flags at all state government buildings flew at half-staff in honor of a member of the Navy from Peoria, AZ, who died March 13 from injuries suffered in Afghanistan on March 10.

CTTC(SW) Christian Michael Pike, 31, was conducting stability operations in Maiwand District, west of Kandahar, the U.S. Defense Department announced March 14.

After being injured, Pike was taken to a U.S. Army hospital in Landstuhl, Germany, where he was pronounced dead. "Pike was assigned to a West Coast-based Naval Special Warfare unit," said LCDR David McKinney, a spokesman for Naval Special Warfare Command.

Governor Jan Brewer ordered flags at government buildings lowered immediately in the hours after the Defense Department's announcement.

"My heart breaks for the family and friends of Chief Petty Officer Christian Michael Pike," the governor stated in a prepared release.

"I ask that all Arizonans join me in thoughtful prayer for CPO Pike, his loved ones and his fellow Navy brothers and sisters," the statement continued.

"Please keep all of Arizona's servicemen and women in your hearts and thoughts. Their service and sacrifice must never be taken for granted."

Pike joined the Navy Aug. 16, 2001, and following training was assigned to the NTTC Corry Station, then the USS Cleveland, according to a biography supplied by the Naval Special Warfare unit in California. In 2007, he moved to a Navy Information Operations Command facility in Georgia before reporting to the Special Warfare unit Jul. 25, 2011.

FEDERAL 100

RECOGNIZES BUSINESS SAVVY ADMIRAL

Official U.S. Navy Photo

RADM David G. Simpson
(Vice Director for DISA)

The one-time communications and information systems director for U.S. Forces-Iraq in Baghdad is bringing his strategic and operational experience home.

As a champion for DOD's Joint Information Environment, RADM David G. Simpson helped build the architecture that supports enterprise email and other department wide services and has been an advocate for enterprise licensing agreements, financial transparency and standardization.

"Dave exemplifies that rare combination of both strong technical skills and business savvy, and his efforts are making a big difference as the department continues to foster innovation during tough financial times," said Dave Wennergren, DOD's assistant deputy chief management officer.

Simpson and this year's other winners were chosen by a select panel of government and industry leasders. The winners include 22 from industry, two from academia, one from state government and 75 from the federal government -- with 56 in civilian agencies, 15 in the defense sector and four from Capitol Hill.

The 2013 winners face persistent budget uncertainty, election-year politics, and IT challenges that have grown more complicated and faster-moving than ever.

Photo by Army SPC Vanessa Davila

ITC Duane King

ABOVE AND BEYOND

By CDR Patrick Honeck, CYBERFOR FEWC

Challenges within the Electro-magnetic Spectrum are rarely understood by most of the population. It requires true professionals, with the right training and experience, to really understand the challenges that surround the sometimes mystical environment known as the Electromagnetic Spectrum (EMS).

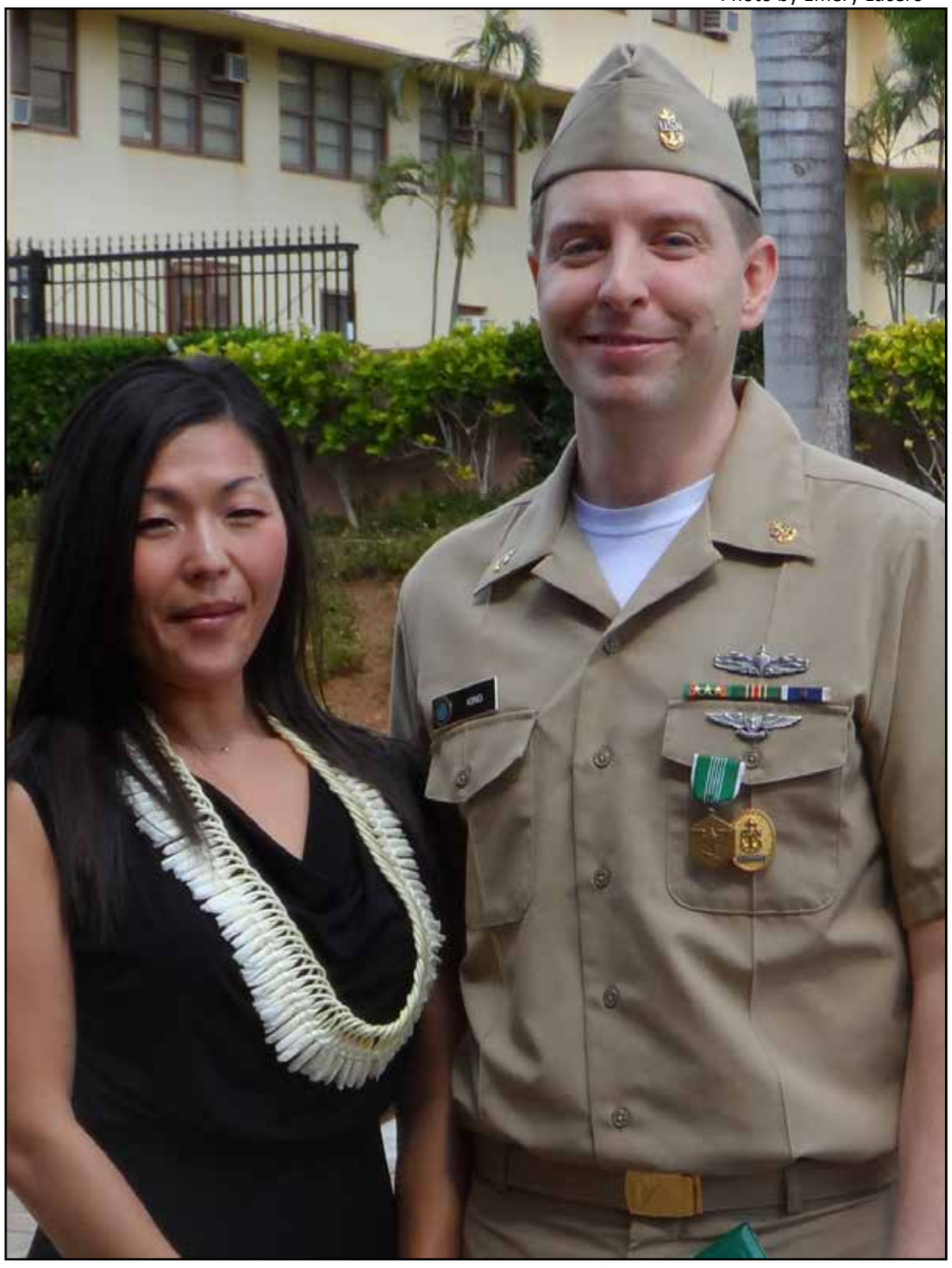
Because the EMS is an environment that can't be readily seen or touched, we often forget it is there.

As a medium that carries most of our unseen data at one point or another it is an amazing asset for productivity and security until it ceases to function the way we want it to. If you have ever endured static on a radio, puzzled over a radar screen that was not showing you what you thought

. . . continued on Page 29

. . . continued from Page 28

Photo by Emery Lucero



ITC Duane and Momoko King

it should, or experienced dropped calls and vanishing text messages on a cell phone, you have experienced small parts of these challenges.

As our world becomes more dependent upon wireless devices (from radars and radios, to smart phones and tablets) the EMS becomes increasingly congested. Much like the expanse of freeway available around the Washington, DC beltway, still at rush hour, it eventually becomes saturated with vehicles to the point of gridlock.

To ensure all of these vital EMS systems operate harmoniously and without electromagnetic gridlock, it increasingly important to have experts on hand to manage and support the invisible energy transporting information through the airwaves.

ITC Duane King is one those essential experts. King was recently recognized for his outstanding and meritorious service as Spectrum Management Program Expert for Joint Task Force (JTF) Guantanamo and Naval Station Guantanamo Bay during a six-month temporary assignment from the Navy and Marine Corps Spectrum Office Pacific (NMCSO PAC), located on Camp Smith, HI.

King was awarded the Army Commendation Medal from Army Brig.Gen. James C. Lettko; deputy commander Joint Task Force Guantanamo for his steadfast efforts to resurrect a severely neglected Spectrum Management Program that had not been updated in more than 10 years.

Assigned to Guantanamo Bay to assess the EMS, train personnel in communications and spectrum support, and ensure operational status of equipment, King exceeded all expectations during his deployment. Demonstrating superior technical expertise, a tireless work ethic, and the can-do attitude of a Navy Chief, he rapidly earned the respect of both leadership and his peers.

With the aid of a spectrum analyzer, King successfully identified 835 undocumented radio frequencies being used by the base and the JTF. Shepherding staff personnel through the spectrum management process, he expeditiously brought both organizations into Department of Defense compliance without disruption of any critical services.

To sustain the procedures and processes he established, King trained and qualified two permanently assigned civilian personnel to serve as Spectrum Managers and another 30 communications personnel in both Spectrum Management and radar planning. His efforts institutionalized sound spectrum management practices that will ensure the Naval Station and the JTF continue to have assured access to the EMS and the critical information systems upon which their missions depend.

King went above and beyond what was expected during his time in Cuba. He improved JTF mission effectiveness and efficiency. His dedication and tireless effort will have positive and enduring effect on thespectrum policies and the personnel of both JTF Guantanamo and Naval Station Guantanamo Bay for years to come. King's achievements are reflections of the Navy and Marine Corps Spectrum Center Command Philosophy: "Mission first, people always".

Official U.S. Navy Photo

NMITC Shows Foreign Officers The Ropes

By Lt. Jason Bruehl, NMITC Public Affairs

DAM NECK, VA – The Navy and Marine Corps Intelligence Training Center (NMITC) welcomed senior Foreign Liaison Officers from Mexico, Peru, Brazil and Chile, and provided a general overview of the various training programs offered at NMITC.

These liaison officers are assigned to U.S. Fleet Forces Command (USFF) under a program designed to help foster a mutual understanding of methods of organization, administration, doctrine, planning and operations between the U.S. and respective partner nations.

The liaison officers were greeted by NMITC Commanding Officer CAPT William Kotheimer, and members of his senior staff. The group met with NMITC's leadership and received a command brief with a discussion on NMITC's courses of instruction and how their graduates are prepared to provide invaluable contributions to the Fleet.

"This visit was a great opportunity to showcase NMITC's mission and training programs with a number of key partner nations," he said. "I am glad we had an opportunity to meet, and I look forward to continued engagements in the future".

Kotheimer led the liaison officers on a VIP tour of the command to show first hand some of the innovative instructional methods being used to deliver course content at NMITC, including the use of technology in the classroom to enhance learning.In particular, the group received overviews of the Navy Intelligence Officer Basic Course (NIOBC), Navy Intelligence Specialist "A" School, and various Intelligence Specialist "C" School courses.

The liaison officers were impressed with the quality of instruction and programs being taught at NMITC. Along the way they had the opportunity to view NMITC's history wall, detailing the progression of U.S. Naval Intelligence and its vital contributions throughout our nation's history, and the Hall of Valor, which honors Navy and Marine Corps intelligence professionals who have fallen in the line of duty.

Kotheimer said he thoroughly enjoyed the opportunity to meet with the liaison officers.

The mission of NMITC is to deliver entry-level, mid-career, and advanced all source naval intelligence training for enlisted and officer students directly supporting Fleet, Navy-Marine Corps team, and intelligence community requirements for trained-and-ready intelligence professionals, to achieve decision superiority.

Flexibility Keeps e-Learning Afloat

By Ed Barker, Naval Education & Training Command Public Affairs

PENSACOLA, FL – The Navy's Web-based training system, Navy e-Learning (NeL), set a record in Fiscal Year 2012 for the most course completions by afloat units.

More than 217,000 course completions were recorded during the year by 191 ships and submarines.

"Working to constantly improve the afloat side of Navy e-Learning, and we are seeing increased usage and better results as this application matures," said Hank Reeves, NeL project director.

"We've seen steady increases in usage and availability each year since the inception of NeL in 2001."

NeL afloat offers more than 1,600 courses, ranging from Information Assurance Awareness training required of all Sailors to hull-specific training for individual units.

The aircraft carrier USS Carl Vinson (CVN 70) was one of the top NeL afloat performers in 2012 with more than 19,000 course completions. LCDR Kevin Halfacre is Vinson's training officer and appreciates the flexibility NeL offers his Sailors.

"Our crew is able to complete all of their required General Military Training (GMT) courses using NeL and that helps us manage our schedule while underway or pierside," said Halfacre.

"We don't have to schedule classes, classrooms or instructors on board," said Halfacre. "The flexibility and 24/7 availability of courses through NeL afloat works very well for us."

The computer server hosting NeL afloat is resident on board each platform and runs independently without a constant Internet connection. When connectivity is available, the server can transfer information back to the shore side for updating Sailors' Electronic Training Jackets (ETJ) and transmitting the latest training and personnel information. NeL software and courseware updates are pushed to afloat units on a monthly basis. Each month, ships receive 50 to 100 new courses via training amendment packages.

"Navy e-Learning is a great tool for Sailors on board aircraft carriers. It allows them to complete required shipboard training such as the Damage Control Petty Officer (DCPO) course, but it also supports their personal and professional development by offering Professional Military Education and foreign language courses," said LCDR Jeffrey Gregor, Aircraft Carrier Training Readiness Officer for Commander, Naval Air Force, U.S. Pacific Fleet.

Although online courses are available on all of the Navy's sea-going platforms, operational limitations can vary system performance throughout the Fleet.

"Due to the nature of the submarine operating environment and bandwidth limitations of submarine communications networks, NeL is challenged to provide the same quality of service experienced by other Fleet Sailors," said Mark Steele, knowledge manager for Commander, Submarine Force Atlantic. "We are optimistic, however, that with hardware upgrades and the development of tailored software solutions, we are headed in the right direction to optimize the NeL experience for our submarine Sailors."

On the ashore side, the NeL environment consists of a comprehensive catalog of distance learning course options available internationally to Active and Reserve component Navy military personnel, DON civilians, contractors, dependents and retirees. The catalog currently contains more than 8,000 courses (including the 1,600 available through NeL afloat), and supports Navy "A" and "C" schools with content and learning management services.

"As NeL continues to grow, we look forward to improved performance from both the shore and afloat versions," said Reeves. "Our ultimate goal is to have the same connectivity and performance for Sailors regardless of where they are located, providing the training that the Fleet needs."

The acquisition effort to modernize Navy e-Learning (NeL) capabilities is called the Enterprise Training Management Delivery System (ETMDS). The ETMDS modernization represents a significant upgrade to existing shore-side NeL capabilities and offers a pathway for introducing additional capabilities in the areas of Total Force workforce management and development. The system is currently in the testing phase.

To visit the full Navy e-Learning catalog, click on the NKO Web site at https://www.nko.navy.mil and after logging in, click on 'Navy e-learning online courses' under the 'learning' tab on the top right of the page.

For more news on the Naval Education and Training Command, visit the NETC Web site at: https://www.netc.navy.mil.

Stories & Photos by George Lammons, NMOC Public Affairs Officer

VALPARAISO, Chile - (Left to right) RDML Brian Brown, commander Naval Meteorology and Oceanography, (COMNAVMETOC), welcomes Alejandro D. Wolff (far right), U.S. Ambassador to Chile, aboard USNS Pathfinder (T-AGS 60) with Marty Ammond, COMNAVMETOC program analyst, and Joseph Goodwin, Pathfinder's master; on a port call. Pathfinder, an oceanographic survey ship, is in Valparaiso as part of Oceanographic Southern Partnership Station. (Photo by Jeff Smith)

U.S. Oceanographic Survey Ship Works with Chilean Navy

USNS Pathfinder (T-AGS 60) visited Valparaíso, Chile's EXPO NAVAL event recently as part as a part of Oceanographic Southern Partnership Station (OSPS) in connection with Expo Naval 2012, the 8th International Maritime and Naval Exhibition and Conference for Latin America. OSPS is an engagement focused on oceanography and hydrographic surveying and the exchange of information between subject matter experts from partnering navies within the U.S. Southern Command region.

The ship, an oceanographic survey ship, and ship personnel participated in the EXPO NAVAL activities to showcase recent and current U.S. Navy and Chilean Navy joint survey operations and new initiatives. The ship activities also included a reception hosted by RDML Brian Brown, commander of the Naval Meteorology and Oceanography Command.

Pathfinder is in Chile at the invitation of the Government of Chile, to continue efforts in assisting the Chilean Navy's Hydrographic and Oceanographic Service (SHOA) to re-survey the seafloor in and around the Bay of Concepcion and Golfo de Arauco - an area greatly affected by the February 2010 earthquake and tsunami.

Both Chilean Navy and U.S. Navy hydrographers and oceanographers will also use this time to share their expertise and learn from one another. This collaborative effort primarily focuses on ensuring safe maritime navigation after a massive natural disaster - and further exemplifies the strong partnership between the United States and Chile.

In October 2010, the U.S. Navy Fleet Survey Team (FLTSURVTEAM) worked with SHOA for two months to re-survey shallow water coastal areas around Talcahuano. During January and March 2011, Pathfinder, with U.S. and SHOA personnel embarked, conducted mid to deep-water hydrographic surveys, and the data collected by both FLTSURVTEAM and Pathfinder will be used to update nautical charts and improve safety of navigation.

Pathfinder is deployed as part of the U.S. Southern Command's Oceanographic Southern Partnership Station.

What Does It Take to be a Flight Meteorologist?

The Naval Oceanography Anti-Submarine Warfare Detachment (NOAD), Whidbey Island, WA, recently established the Flight Meteorologist Program (FMP) to support tactical flights on P-3s.

The program also gives AGs the opportunity to gain first-hand experience on Maritime Patrol Reconnaissance Aircraft (MPRA).

LTJG Jason Ehlenberger was the first to qualify and earn his Naval Aviation Observer (NAO) badge. Five others in his detachment are working toward their qualification, logging over 100 hours of flight time.

Personnel must complete water survival training, qualify as naval air training and operating procedures observers, and fly a minimum of 60 hours to qualify.

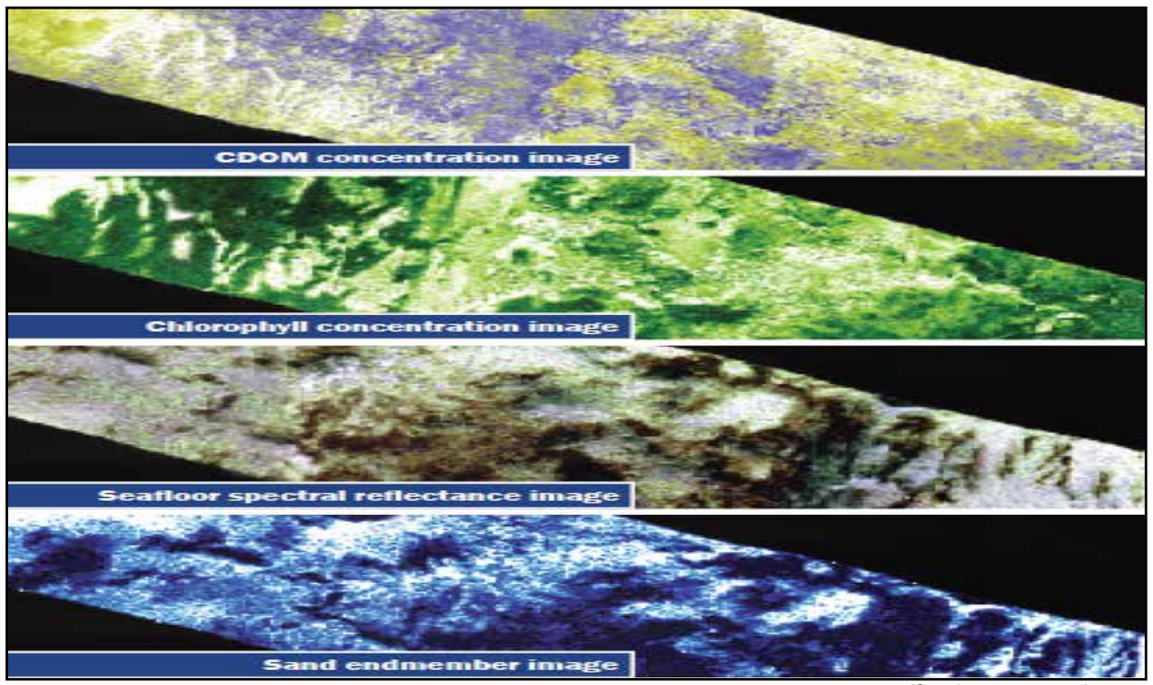
Navy Explores New Airborne Mapping System

RDML Brian Brown, Commander, Naval Meteorology and Oceanography Command, and other personnel, received their first look at the Navy's latest airborne lidar mapping and charting system at Stennis Airport.

The Coastal Zone Mapping and Imaging Lidar (CZMIL), system has replaced the retired Compact Hydrographic Airborne Rapid Total Survey system that was used for the past nine years.

The new CZMIL is undergoing testing and evaluation by the Naval Oceanographic Office Airborne Coastal Surveys Branch before deployment early next year.

The system is mounted in a DC-3 aircraft, specifically designed for the testing of sensors. This configuration provides an opportunity for several people to experience the data collection and undergo system operation training at once. The new system is capable of simultaneously collecting hydrographic and topographic data along with Red, Green, Blue (RGB) and hyperspectral imagery. It is specifically designed to work in more turbid water than the previous system.



Official U.S. Navy Photo

Unmanned Underwater Vehicle Goes UA

Naval Oceanography Mine Warfare Center based at Stennis Space Center, MS, lost contact with one of its Remus 100 Unmanned Underwater Vehicles (UUV) in the Gulf of Mexico near Panama City and Biltmore Beach in Florida during a training exercise on Thursday night.

The UUV poses no danger or threat to the public or sea life. The UUV is a battery powered vehicle that is programmed to follow an underwater search pattern using low power sonar energy to look for objects on the sea floor. The last contact with the vehicle showed it heading north, so it has a good possibility of reaching shore. However, it also could be adrift in the gulf.

Official U.S. Navy Photo

STENNIS SPACE CENTER, MS - (Left to right) AG2 Christopher Kyall of Fleet Survey Team briefs RDML Gerd Glang, Director of NOAA's Office of Coast Survey during a visit to the Naval Oceanographic Office at Stennis Space Center. Also pictured is Kyall's commanding officer, CDR Ron Shaw.

Navy Relates to Hawaiian Middle School

The Joint Typhoon Warning Center (Joint Typhoon WRNCEN) was recognized at the 11th Joint Venture Education Forum (JVEF) for the command's close relationship with Moanalua Middle School.

The JVEF is a cooperative venture between the U.S. Pacific Command and the Hawaii Department of Education that promotes interaction between the military community and state educators, allowing issues pertaining to the military and the public school system to be raised and resolved.

JTWC and Moanalua Middle School have enjoyed a 20-year partnership that has included reading, teaching earth science, rebuilding the school's library and mural painting.

‘Better Access to Cyberspace’ Awarded to 19-member FCC Team

From Commander, U.S. Fleet Cyber Command/U.S. 10th Fleet Public Affairs

The U.S. Fleet Cyber Command (FCC) Information Technology and Governance Team was announced as a winner of the 2013 Department of the Navy (DON) Information Management/ Information Technology (IM/IT) Excellence Award at the Armed Forces Communications and Electronics Association’s West 2013 conference in San Diego.

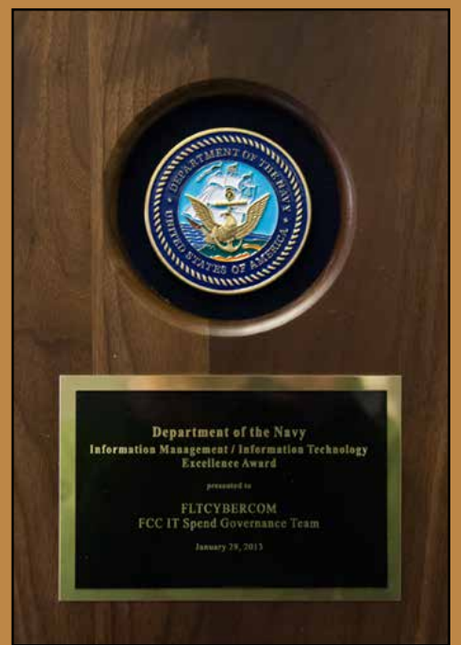
The annual DON IM/IT Excellence Awards recognize IM/IT teams, projects, and individuals that have helped to transform the Navy and Marine Corps through information technology.

The award recognizes the FCC team’s dedicated work in creating new processes and ongoing analysis that facilitated the approval of over 800 IT investment requirements for Navy funded, Navy and Marine Corps Intranet/Continuity of Service Contract (NMCI/CoSC), and nationally funded IT procurement requests.

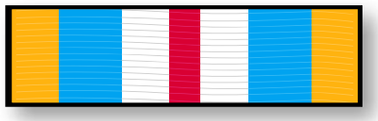
“Our 19 member team can be proud of their accomplishments over the past year that benefit not only the command, but the Navy as a whole by creating efficiencies that maximize resource utilization - an ever more critical necessity in this challenging fiscal climate,” said Kevin Cooley, FCC’s chief information officer and executive director.

“We’re proud of the team’s hard work that has enabled FCC leadership to make decisions during the past year to avoid duplicate projects, ensure consistency throughout the domain, and identify new avenues to pursue IT efficiencies,” said team leader and member Neal Miller, FCC Deputy Chief Information Officer for Mission Assurance.

Importantly, these efficiencies aid FCC in fulfilling its goal of providing Navy and Joint commanders with an operational advantage by assuring access to cyberspace and confident command and control, preventing strategic surprise in cyberspace, and delivering decisive cyber effects.



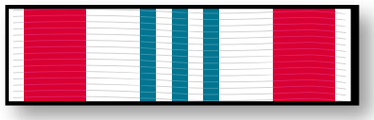
The 2013 Department of the Navy (DON) Information Management/Information Technology (IM/IT) Excellence awardees assigned **to Ft. Meade, MD and featured in the (Left photo, left to right) Amanda Jordan, Customer Service Representative and Process Improvement Analyst; Michael Kegley, Web Subject Matter Expert and Technical Process Lead; Allen Seward, Contracts Subject Matter Expert; Quintin Hudgens, Customer Service Representative. Missing are Kevin Cooley, CIO/ED and Cathy Porter, N6 Representative. Awardees assigned to Joint Expeditionary Base Little Creek-Fort Story and featured in the (Right photo, front row from left to right) Neal Miller, Deputy CIO; Deniese Cobbins, IT Resource Manager; Charlene Plaine, OSD Certification. (Back row) Shawn Garrow, Enterprise Architecture(EA); Michael Miller, EA; Carlos Parter, Legacy Networks/Server Compliance; Teresa Duvall, Section 508 Compliance/ Ginger-Cohen Act. Missing are Howell Carter, Legacy Networks/Server Compliance; Anwahe Dubique, IT Budget/NITESTAR; Tracy Scherman, IT Budget/NITESTAR; Jerri Baeumel, Support Services; Alan Rickman, Information Assurance (IA); Freddie Blaser, IA; Randy Summers, DITPR-DON/DAMDS/FAM/Enterprise Licensing. (Official U.S. Navy Photos)**



CAPT Jill Newton, NIOC Maryland

LEGION OF MERIT

CDR Debra Lankhorst, FLTCYBERCOM
CAPT Veronique Streeter, NCTS FAR EAST

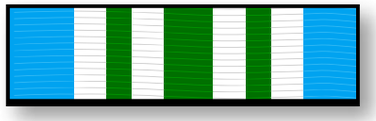


DEFENSE MERITORIOUS SERVICE MEDAL

CTRC Joey Alexander, NIOC Maryland
CTT1 Keenan Billingsley, NIOC Hawaii
CWO3 James Bryars, NIOC Maryland
LT Richard Buckley, NIOC Hawaii
LCDR Brian Burrow, NIOC Maryland
CTRC Wayne Bye, NIOC Maryland
CTIC James Chaffin, NIOC Hawaii
LCDR Craig Fowler, NIOC Maryland
CTIC Brandon Granger, NIOC Menwith Hill
CTIC Thomas Hirzel, NIOC Texas
CTT1 Bryan Johnson, NIOC Maryland
CTR1 Patricia Madigan, AROCC
CDR Timothy May, CSG Afghanistan
CTNC Max Narango, NIOC Maryland
CTTC Christopher Noltee, NIOC Colorado
CDR Neal Nottrott, NIOC Maryland
CTRC Sheryl Reeder, NIOC Maryland
CTRC Michael Russo, NIOC Maryland
CTRC Michael Shanks, NIOC Texas
CDR David Van Brunt, NIOC Maryland
CTNC Brian Waggoner, NIOC Maryland

MERITORIOUS SERVICE MEDAL

ITCM Frank Cannizzaro, NCTS Jacksonville
CDR Cameron Carney, FLTCYBERCOM
CAPT William Darling, NR NNWC
LT Jamie Davis, NIOD Jacksonville
CMDCM Joseph Giustiniano, NCTS San Diego
CAPT Brian Hastings, NR NIOC Maryland
CDR John Johnson, FLTCYBERCOM
LCDR Jeffrey Kenney, NCWDG
CDR Reginald King, NR NIOC Hawaii
CDR Christopher Malone, NETWARCOM
CDR Joseph McAlexander IV, FLTCYBERCOM
ISCM Thomas Nank, CYBERFOR FID WA
LCDR Thomas Ryan, NCTAMS PAC
CDR David Wojda, FLTCYBERCOM
CDR Michelle Young, NCTAMS PAC



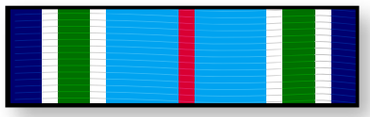
JOINT SERVICE COMMENDATION MEDAL

CTI1 Edgar Bahamon, NIOC Texas
LTJG Kayleigh Biven, NIOC Texas
CTT1 David Blausey, NIOC Menwith Hill
CTI2 Kathryn Claussen, NIOC Texas
CWO3 Edwin Combs, NIOC Maryland
CTI1 Sarai Cordova, NIOC Texas
CTR1 David Dent, NIOC Menwith Hill
CTN1 William Erickson, NIOC Texas
CTT1 Kersanda Estes, NIOC Menwith Hill
CTI2 Nicole Frederick, NIOC Texas
LTJG Nyere Grant, NIOC Maryland
IT1 Brooke Hejl, NIOC Texas
CTT1 Andrew Hernandez, NIOC Colorado
CTR2 Christopher Hines, NIOC Maryland
CTI1 Lindsay Hoying, NIOC Menwith Hill
CTR2 Jaella Humphrey, NIOC Misawa
CTI1 James Johnson, NIOC Maryland
CTR1 Erick Killian, NIOC Maryland
CTM2 Paul Kim, NIOC Hawaii
CTR2 Shanice Liwanag, NIOC Misawa
CTN2 Clayton Lumpkin, NIOC Texas
CTI2 Jesus Martinez, Joint Task Force
CTI2 Christopher McGowen, NIOC Hawaii
CTR1 Justin Mitchell-Hynd, NIOC Maryland
CTT1 Brian Mixon, NIOC Colorado
CTR1 David Morales, NIOC Texas
CTN1 Priscilla Morris, NIOC Texas
CTR1 Amy Palmer, CSG Joint Staff
YN2 Patrick Parker, NIOC Maryland
LT David Perez, NIOC Misawa
CTN1 Marcella Rax, NIOC Texas
CTI1 Joseph Reynolds, NIOC Georgia
CTI1 David Rodriguez, NIOC Texas
CTI1 Bonita Sabia, NIOC Hawaii
CTR2 Kyle Scarborough, NIOC Menwith Hill
CTI1 Jennifer Sizemore, NIOC Texas
CTR2 Shauntell Talbert, NIOC Hawaii
YN2 Kareem Turnbull, NIOC Maryland
CTI1 Traca Tuthill, NIOC Maryland
CTN2 Joseph Vieke, NIOC Maryland
CTR2 Chad Welsh, NIOC Hawaii

NAVY AND MARINE CORPS COMMENDATION MEDAL

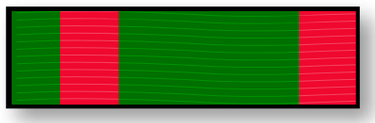
LT Dorian Acker, NIOC Norfolk
LT Jordan Adler, FLTCYBERCOM
LT Charles Ahn, NCWDG
LT Christopher Allen, NIOC Norfolk
CTM1 Anthony Anderson, NCWDG
ITC Peggy Arnold, CMS TRA TEAM Far East
LSC Mamerto Bolado, NIOC Yokosuka
CTRC Mahlon Braden, NIOC Hawaii
CECS Alexander Bradshaw, NCTS Naples
LT Ryan Breckenridge NIOC Hawaii
CTRC Byron Brooks, NCWDG
ITCS Darrell Brown, NCTS Bahrain
CTN1 Derick Bryant, FLTCYBERCOM
LT Tyler Carr, NCWDG
CTIC Kelly Chambers, NIOC Maryland
ITC Adrienne Charles, NETWARCOM
CTTC Michael Cibor, NIOC San Diego
LCDR Ricard Clement, NCTAMS LANT
LSC Yvonne Cole, NCTS Sicily
LCDR Richard Colli, NR CYBERFOR OPS
CTTC Woodrow Copen, Jr., NIOC Norfolk
ITC William Coston, NCTAMS LANT
ITC Ryan Courton, NCTS Naples
CTR1 Mark Crane, II NIOC Maryland
CTTC Danielle Crowley, NIOC San Diego
ITC Alison Czuhajewski, CMS TRA TEAM Honolulu
LCDR Tuan Dang, NCTS San Diego
LSC Brenda Dasher, NCTAMS PAC
CEC Wilbert Davis, NCTS Naples
LTJG Shawn Dawson, NCTAMS LANT Norfolk
CWO4 Keith Denton, FLTCYBERCOM
ITCS Cathy Dorgan, NETWARCOM
LTJG Kevin Dougherty, NIOC Hawaii
CTMC John Earnshaw, NCWDG
CTN1 Keith Elinkowski, NCWDG
IT1 Vonetta Ellison, NCTS Bahrain
IT1 Charles Ellison, Jr., NIOC Maryland
LCDR Benedict, Eu, NR COMTENTHFLT
ITC Anthony Ferrara, NCTAMS LANT DET Souda Bay
CTR1 Michael Fletcher, NIOC Maryland
CTRC Andy Fowler, NIOC Georgia
CTR1 Alexis Gallegos, NIOC Maryland
CTRC Daniel Gammon, NIOD Jacksonville
CWO2 Eric Godlewski, NIOC Hawaii
ITC Leslie Gonzalez, NCTS Naples
ISC Patricia Grantham, NCWDG
ET1 Larry Hale, NCTAMS LANT
CTN1 Kevin Hall, NCDOC
CTMCM Donald Harris, NIOC Norfolk
LCDR Kenneth Helman, NR NIOC Hawaii
LCDR Christina Hines, NETWARCOM
CTMC David Hurley, FLTCYBERCOM
ET1 Michael Ignoffo, NCTS Naples
LT Robert Ireland, CYBERFOR Virginia Beach
YNC Marcus Jackson, NCWDG
CTNC Joseph Jaramillo, Jr., NCDOC
LCDR Ventura Jimenez, Jr., NR NIOC Hawaii
CTI1 Adam Justice, NIOC Maryland
LCDR Raymond Kenning, NR NCDOC
LT Richard Kidder, Jr., NCTS Naples
ITC Clifford King, NCTS Naples
CTNC Matthew Kopczynski, FLTCYBERCOM
LCDR Linda Laws, NCTS San Diego
CTNC Deaden Lee, NCWDG
IT1 William Lee, NCTS Sicily
LCDR Jeremy Livingston, NETWARCOM
LSCS Jose Madrigal, NCTAMS LANT DET Rota, Spain
CTMC Christopher Manfredi, NIOD Groton
IT1 Robert Manyak, NCDOC
CTMCS Franklin Marcus, Jr., NIOD Groton
YNCS Hercules Martin, NCMS Washington
ITC Althea McCalla, NETWARCOM
LT George McLaughlin, NAVIOCOM Norfolk
CTR1 Gerard Miesel, NIOC Pensacola
YN1 Heather Montgomery, NIOD Jacksonville
LCDR Matthew Myers, CYBERFOR FIAF DET Norfolk
CTR1 Stephen Noreika, NIOC Whidbey Island
CTT1 Benjamin Northcutt, NIOC Hawaii
CTNC Beulah Parks, CYBERFOR Virginia Beach
CTIC Christopher Patti, NIOC Maryland
YNC Kraag Pedersen, NCTS Naples
CWO3 Harold Phillips, NCTAMS LANT Det Hampton Roads
LT Aaron Pickett, NCWDG

CTI1 Michele Pineira, NIOC Misawa
LS1 Christopher Pineza, NCTS Sicily
ET1 Jerry Ramm, NCMS Washinton, DC
ETC Peter Reniere, CYBERFOR Virginia Beach
IT1 Gincie Rhodes, NCDOC
CECS Ariel Ricasata, NCTAMS LANT
YN1 Angela Robinson, NIOC Bahrain
ITCM Michael Rufa, NMCSO LANT Norfolk
ITCS Jeffrey Rumbold, NCTAMS PAC DET Puget Sound
LT Michael Schaefer, NIOC Norfolk
ITC Tyree Scott, NCDOC
CTT1 Ebony Seymoure, NIOC San Diego
ITCS Marion Shawbell, NCTAMS PAC
CTT1 Raymond Sherrier, NIOD Jacksonville
ETCS Billy Smith, NCTS Naples
ITC Jonathan Sneller, NCTAMS LANT
CTI1 Jason Snyder, NIOC Misawa
IT1 Penny Steenrod, NCTAMS LANT
YNC Amanda Stickler, NIOC Hawaii
ITC Roger Summerville, NCTS Naples
ITCS Tyrone Tate, CMS TRA TEAM San Diego
ITC LaMichele Tyson, NCMS Wash
CTR1 Randy Vandervoort, NIOD Digby
ITC Woodrow Wagoner II, NCTS Bahrain
LCDR Ronald Waldon, NR NAVNETWARCOM
CTI1 Joshua Weaver, NIOD Jacksonville
YN1 Candice White, CYBERFOR Virginia Beach
IT1 Jonathan Wilk, NCTS Sicily
LT Luke Wilson, NIOC Georgia
LCDR Robert Woodruff III, NIOC Hawaii



JOINT SERVICE ACHIEVEMENT MEDAL

CTI2 Neva Anderson, NIOC Texas
IT3 Desmond Andrews, NIOC Misawa
CTI2 Patrick Backman, NIOC Maryland
CTT2 Michael Bogan, NIOC Texas
CTR2 Vanessa Brieden, NIOC Maryland
CTR2 Samantha Brown, NIOC Texas
CTR3 Patricia Burke, NIOC Texas
CTT2 Terrance Burrell, NIOC Texas
CTI2 Alan Castle, NIOC Texas
CTR1 Eric Cope, NIOC Texas
CTIC Matthew Culbertson, NIOC Texas
CTR1 Richard Durant, NIOC Texas
CTT2 Sephra Dyall, NIOC Colorado
CTI2 Gregory Goerge, NIOC Maryland
CTI2 Adrienne Griffith, NIOC Texas
CTN3 Leroy Hatcher, NIOC Texas
CTI3 Nicholas Helak, NIOC Texas
CTR2 Sara Hewes, NIOC Texas
CTM3 Stephen Hill, NIOC Maryland
CTR3 Raheem Hines, NIOC Texas
CTI3 Vanessa Horne, NIOC Texas
CTT2 Nicholas Hummel, NIOC Maryland
IT3 Austin Hutchens, NIOC Maryland
CTI2 Rochelle Jackson, NIOC Texas
CTI2 Justin Jolley, NIOC Maryland
CTI2 Laura Kembel, NIOC Georgia
CTI2 Stephanie Lynner, NIOC Georgia
CTI2 Katharine Morse, NIOC Maryland
CTR3 Dalicia Mosley, NIOC Hawaii
YN1 Mathew Olson, NIOC Menwith Hill
CTT2 Kyle Overton, NIOC Colorado
CTI2 Alexander Proulx, NIOC Maryland
CTN2 Rederi Rantayo, NIOC Texas
CTI2 Dani Ridgway, NIOC Texas
CTM2 Robert Rohm, NIOC Maryland
CTR3 Kayla Rosche, NIOC Menwith Hill
CTI2 Justin Schritter, NIOC Maryland
CTN3 Aaron Serwa, NIOC Texas
CTI3 Rebecca Stone, NIOC Maryland
CTI1 Karl Swarner, NIOC Texas
CTN2 Denton Sweat, NIOC Texas
CTN2 David Tompkins, IOC Texas
CTI3 Vincent Torrente, NIOC Texas
IT3 David Trent, NIOC Maryland
CTI1 Joshua Voyles, NIOC Texas
CTI2 Alexa Whiteway, NIOC Maryland
CTI2 Ellen Wilson, NIOC Hawaii
CTI2 Jessica Wilson, NIOCTexas



NAVY AND MARINE CORPS ACHIEVEMENT MEDAL

IT1 Johanna Albarran, NCTS Naples
IT2 Stephanie Albers, NCTAMS PAC
CTR2 Morgan Alexander, NIOC Maryland
IS2 Qasim Ali, CYBERFOR FID Fallon
IT2 Luis Alonso, NCTAMS PAC
IT2 Mohammed Alshibani, NCTAMS PAC
CTTSN Ameline Alvarez, NIOC Hawaii
IT1 Richard Amrhein, NETWARCOM
CTN1 Chad Arnold, NIOM Pensacola
IT2 Christopher Atkins, NCTAMS LANT DET Hampton Roads
LTJG Joseph Atzenbeck, NIOC Hawaii
IS2 Erica Avery, NIOC Hawaii
IT2 Jeffrey Barnett, NCTAMS LANT DET Rota
ET3 Timothy Baur, NCTS Bahrain
IT1 Geneson Bautista, NAVCYBERFOR DET San Diego
ET3 Trisha Baxter, NCTAMS LANT
LT John Bayer, NAVCYBERFOR Virginia Beach
IT2 Jennifer Bean, NCTS Sicily
CTR2 Keith Beaner, NIOC Hawaii
CTM3 John Beasley, NAVIOCOM Hawaii
CTN2 Luke Becker, NCDOC
IS2 Melissa Bell, NCTAMS LANT
MA2 Christopher Benner, NIOC Hawaii
CTM1 Stephen Bennett, NIOD Groton
CTR1 William Blevins, NIOC Georgia
IT1 Robert Blevins, Jr., NCTAMS LANT Norfolk
IT1 Jason Bond, NCTAMS PAC
CTT1 Keith Boyd, NIOC Hawaii
IT3 Melissa Brick, NCTS San Diego
CTI1 Roderick Broach, NIOC Hawaii
ITC Kevin Bryars, NCTS Bahrain
LS2 Justin Burdett, NIOC San Diego
CTR2 Ryan Burnett, NIOC Hawaii
CTM1 Melanie Bynoe, NCWDG
ITC Daniel Cacciatore, NCTS San Diego
CTN1 Joseph Caddy, NIOC San Diego
IT2 Cassey Carlson, NAVIODET Seoul
MC2 Joel Carlson, NIOC Sugar Grove
CTI1 Thomas Carter, NIOC Georgia
CTR2 Ryan Cassady, NCWDG
CTI1 Alyssa Chubbuck, NIOC Hawaii
IT2 Joshua Claggett, NCWDG
ET2 Aaron Cole, NCTS Naples
CTN3 Bradford Collier, NIOC Maryland
IT2 Tameka Colvin, NCTS Bahrain
IT1 Landin Comins, NCTS San Diego
YN3 Christopher Coogan, NIOC Yokosuka
CTM1 Benjamin Cozort, NIOC Hawaii
IT1 Kevin Crisco, NCTAMS LANT DET Hampton Roads
ET1 Michael Custodio, NCTS Far East
CE1 Stuart Dahl, NCTAMS LANT Norfolk
CTI2 Christopher Daniels, NIOC Hawaii
CTM2 Ryan Davidson, NIOC Hawaii
CTR2 Derek Davis, NIOC Hawaii
YN2 Anthony Deel, NIOC Hawaii
IT1 Michael Delutri, FLTCYBERCOM
CTR2 Michael Desrosier, NIOC Bahrain
IT1 Douglas Dubuque, NCTAMS PAC DET Puget Sound
IT1 Arthur Dunford, NCTS San Diego
IT2 Eric Durrett, NCTAMS LANT
CE2 Adam Dye, NCTS Naples
CTR2 Matthew Earhart, NCWDG
IT2 Amber Eastman, NCTAMS PAC DET Puget Sound
ET2 Kenneth Eaton, NCTS San Diego
IT1 Ana Eskharia, NCTS Naples
IT3 Enrique Espinozacarvaja, NCDOC
LS2 Gilberto Esteves, NIOC Misawa
IT1 Jacquelyn Fitzpatrick, NCTS San Diego
CTI1 Lakisha Flanagan, NIOC Bahrain
CTT2 Michael Foster, NIOC Maryland
CE1 Dhafir Freeman, NCTAMS LANT DET GTMO
CM1 Samson Freesmeier, NCTAMS LANT Norfolk
CTR1 Nicholas Gaines, NIOD Jacksonville
IT2 Kent Galloway, NCTS Bahrain
IT2 Christopher Gardner, NCTAMS PAC DET Puget Sound
IS2 Lisa Garisto, NIOC San Diego
IT1 Delvon Garrett, CYBERFOR DET San Diego
IS2 Stephen Garza, CYBERFOR FID Fallon
ET3 Tyler Glab, NCTS Bahrain
CTM1 Jeffrey Golden, NIOD Groton
MASN Joshua Goldsmith, NIOC Sugar Grove
ITC Abel Gonzales, NCTS San Diego
IT1 Kassidy Gordon, NCTAMS LANT NMCI DET Norfolk
CTT1 Daphane Green, NIOC Hawaii
IT1 Timothy Green, NCTS Naples
IT1 Vernadean Green, NCTS Naples
LTJG Joel Hamner, NIOC Hawaii
IT3 Jeremy Hargrove, NCTS FE DET Sasebo
LT Althea Harris, NCTAMS LANT
CTI1 Matthew Harris, NIOC Georgia
IT2 Stanley Harris, NCTS Naples
CTM3 Patrick Hartnett, NIOC Hawaii
BU2 Micheal Helms, NIOC Sugar Grove
LTJG Jeanna Henderson, NIOC Hawaii
CTN2 David Hennessy, NIOC Pensacola
CTI1 Brandy Hensley, NIOC Bahrain
IT2 Courtnie Hentley-Ward, NCTS San Diego
ET2 Corey Herget, NCTAMS PAC DET Puget Sound
CTT1 Matthew Hess, NIOC Hawaii
LS2 Heather Higdon, NCTAMS PAC
YN3 Larrece Hills, NCTS Naples
CTR2 Kimberly Hines, NAVIOCOM Maryland
ET2 Braxton Holes, NCTAMS LANT Norfolk
CTR2 Jonnise Hopwood, NIOC Bahrain
YN2 Jennifer Hoskins, NIOC Misawa
CTI1 Lindsay Hoying, NIOC Menwith
FT2 Daniel Hrushka, NCTS Naples
ITSN Cheston Hulett, NCTS Sicily
ETC Christopher Jasmer, NCTS Bahrain
OS2 Tina Jennings, NCTAMS LANT Norfolk
CTRC Kwesi Jernigan, NIOC Hawaii
IT2 Deann Jessinia, NCTS Bahrain
ET3 Casey Johnson, NCTS Bahrain

CTN1 Charles Jones, NIOC Norfolk
ENS Lynne Jones, NETWARCOM
IT2 Adam Jorden, NCTS Naples
ET2 Ashley Kempton, NCTAMS PAC
CTR2 Erin Kidd, NIOD Digby
IT1 Mark Kime, CYBERFOR DET San Diego
ET2 Peter King, NCTAMS LANT DET Rota Spain
ET2 Matthew Knight, NCTS Bahrain
CTR2 Austin Kolar, NIOC Menwith
IT2 Latishia Kollie, NCTAMS LANT DET Hampton Roads
IT1 Jesse Konell, NCTAMS LANT DET Hampton Roads
IT2 Janice Kook, NCTAMS PAC
NCC Shannun Lamorte, NIOC Norfolk
IT2 Brendan Lane, NIOC Yokosuka
ITC Will Lee, NCTAMS LANT
CTN2 Noah Leonard, NIOC Hawaii
CTR2 Tyler Lesser, NIOC Misawa
IT2 Yongze Liu, NCTAMS LANT NMCI DET Norfolk
IT2 Dong Logan, NCTS Naples
CTN1 Jason Lois, NCDOC
OS2 Sarah Lopez, NCTAMS LANT
ITC Sheila Maison, NCTAMS PAC
IT2 Marco Mares, NCTS San Diego
CTR1 Andres Martinez, III NIOC Yokosuka
ITC Gregory McCray, Jr., NCTS Naples
IT3 Justin McManaway, NCTAMS LANT
IT1 Jayson Mendez, NCTS San Diego
CTIC Yves Michaud, NIOD Jacksonville
CTR1 Matthew Miller, NIOC Hawaii
IT1 Ryan Miller, NCTS San Diego
CTN2 John Moleskey, NIOC Pensacola
ET2 Harry Moody, NCTAMS LANT
IT1 Matthew Moore, NCTAMS LANT NMCI DET Norfolk
CTRC Jonathon Morgan, NIOC Pensacola
CTI2 Michelle Morgan, NIOC Hawaii
CTR3 Alexianna Morton, NIOC Misawa
IT2 Christopher Mullen, NCTS Bahrain
IT2 Ashley Myers, NIOC Hawaii
IT2 Tamara Namduang, NIOC Hawaii
ET2 Ryan Nash, NCTS San Diego
IT2 Hung Nguyen, NCTS Naples
ET1 Stephen Nickle, NCTS Bahrain
CTN2 Steven O'Neal, NCWDG
CTM1 Rebecca O'Neil, NIOC Norfolk
YN2 Karli Odomes, NIOC Hawaii
CTRSN James Osburn, NIOC Hawaii
CTI1 Challace Pair, NIOC Hawaii
ET3 Albert Palmer, NCTAMS LANT
ITC Gregory Pearce, NCDOC
CTN3 Ryan Petgrave, NIOC Maryland
CTT1 Matthew Poll, NIOC Yokosuka
CE1 Alexander Prades, NCTS FE DET Atsugi
IT1 Aaron Price, NETWARCOM

IT1 Quantrel Pringle, NCTAMS LANT NMCI DET Norfolk
IT2 James Puncel, NCTS FE DET Atsugi
ETC Ricardo Quintana, NCTS Bahrain
IT1 Alana Raj, NCTAMS LANT
MA3 Kristopher Rakes, NIOC Hawaii
IT3 Kelsey Rathbun, NCTS Bahrain
CTTC Christin Rees, NIOC Norfolk
LTJG Beau Reimer, NIOC Maryland
IT1 Terry Richart, Jr., NCTAMS LANT DET Hampton Roads
CTR2 Gear Robinson, NIOC Hawaii
CTI1 Jeffrey Robinson, NIOD Kaneohe Bay
IT2 Jessica Rodriguez, NCTS Naples
IT2 Martin Rodriguez, NCTAMS PAC
IT2 Jomar Romero, NCTS San Diego
ITC Oneika Rossdavis, FLTCYBERCOM
IT2 Albertjulian Salvador, NCTS Naples
IT3 Nathan Sanchez, NCTAMS PAC
CTN2 Terrence Savala, FLTCYBERCOM
IS3 Garrett Schoonover, NAVIOCOM Maryland
CTT1 James Scott, NIOC Hawaii
IT2 Todd Shanley, NCTS Sicily
CTR2 Abigail Shaw, NIOD Digby
ITC John Sheehy, NCTAMS LANT Norfolk
CTR1 Nathan Shutt, NIOC Bahrain
IT2 Sandra Silva, CYBERFOR DET San Diego
IT3 Kyle Simmons, NCWDG
CTI1 Angela Sinn, NIOC Hawaii
CTT1 Kenneth Slaten, NIOC Georgia
IT2 Celio Soto, Jr. NCTS Naples
IT2 Leticia South, NCTS San Diego
LT Richard South, NCTAMS LANT Norfolk
IT2 Bethanie Spang, NCTS Jacksonville
OS1 Calvin Speed, Jr., FLTCYBERCOM
CTI1 William St. Andre, NIOC Misawa
IT1 Joanne Stanley, NIOC Norfolk
IT1 Patrick Stanley, NCTAMS LANT NMCI DET Norfolk
CTR1 Ian Stocking, NIOC Menwith Hill
CTN2 Alexis Storey, NIOC Georgia
CTN2 Christopher Stover, NCDOC
IT3 Kevin Sturgill, FLTCYBERCOM
IT3 Phillip Swartzlander, FLTCYBERCOM
IT1 James Taylor, NCTAMS PAC
IT2 Gregory Thompson, NCTAMS LANT
LT Christopher Tighe, NIOC San Diego
IS3 Adam Tisch, NIOC Maryland
YN2 Jordan Toellner, NIOC Maryland
CTI2 Micala Troeger, NIOC Georgia
IS3 Jeffery Turner, CYBERFOR FID Fallon
CTI2 Matthew Twitty, NIOC Maryland
MA2 Sean Twyman, NIOC Hawaii
IS1 William Urpsis, CYBERFOR FID Washington
IT3 Lyndon Vanluesauls, NCTS Sicily
ET1 Matthew Vechik, NCTS Naples

ET2 Edisa Villarrealcabal, NCTAMS LANT
CTN1 Patrick Voight, NCDOC
CTR1 Christopher Wanner, NIOC Misawa
ITC Larry Ward, NCTSCU DET PAX River
IT1 Darris Watkins, CYBERFOR Virginia Beach
CE2 Dwayne Watson, NCTS Naples
CTT1 Christopher Watt, NIOC Colorado
IS1 Ian Westad, CYBERFOR FID Washington, DC
IT1 Haven White, FLTCYBERCOM
ITC Regina White, NCTS Guam
IT2 Mark Wilkins, CYBERFOR DET San Diego
ITSN Jaymes Williams, NCTAMS LANT
CTT1 Pearce Wilson, NIOC Yokosuka
CTMCS Duain Woodruff, FLTCYBERCOM
CTR2 Jeffrey Worcester, NIOC Menwith Hill
CTR3 Grady Wright, NCWDG
CTI1 Ian Wyatt, NIOC Menwith Hill
CTT1 Alvinna Young, NAVIOCOM Norfolk
CTM2 Cole Younger, NIOC Yokosuka
IT2 Crisogono Zavalapena, NCDOC

MILITARY OUTSTANDING VOLUNTEER SERVICE MEDAL

IT2 Gloria Fisher, NCTAMS LANT Norfolk

IT3 Kimberly Godwin, CYBERFOR FID Washington, DC
IT1 Binal Jones, CYBERFOR Virginia Beach
IT1 David King, CYBERFOR DET San Diego
CTN1 Justin Mitchell, NIOC Pensacola
ISC Kimberlain Rucker, NIOC Norfolk
ET2 Edisa Villarrealcaballero, NCTAMS LANT
IT2 Winora Whatley, CYBERFOR DET San Diego

MERITORIOUS CIVILIAN SERVICE AWARD

Mr. James Clark, FLTCYBERCOM
Ms. Sharon Shaw, CYBERFOR Virginia Beach
Mr. Charles Tabor, CYBERFOR Virginia Beach

CIVILIAN LENGTH OF SERVICE AWARDS

Charles Tabor, CYBERFOR Virginia Beach - 43 Years
James Clark, FLTCYBERCOM – 42 Years
Louis G. Noah, NCTAMS LANT – 40 Years
Robernette A. Turner, NCTAMS LANT – 20 Years
Mia C. Lee, NCTAMS LANT Det Hampton Rds – 10 Years
Laura L. Quezada, NCTAMS LANT Det
Hampton Rds – 10 Years

Nomination Alone, Humbles Sailor

By MC1(IDW/SW/AW) Elizabeth L. Burke, NETWARCOM Staff Journalist

ITC Dawn Arnold, currently assigned to Commander, Naval Network Warfare Command (NETWARCOM), was recently nominated for the prestigious Master Chief Anna Der Vartanian Leadership Award in the Senior Enlisted category for 2013.

The CAPT Joy Bright Hancock Leadership awards recognize one senior officer and one junior officer, while the Master Chief Anna Der Vartanian Leadership awards, honor one senior enlisted and one junior enlisted service member. The awards were established in 1987 and honor visionary leadership of service members whose ideals and dedication foster a positive working environment by reinforcing and furthering the integration of women in the Navy.

Arnold, a native of Pueblo, CO, joined the Navy in August 1994 as a Data Processing Technician and converted to the Radioman rating in 1997. During a tour in Washington, DC, she was selected as Deputy Chief of Naval Operations and Chief of Naval Operations Junior Sailor of the Year in 2000 and subsequently 2005 Sailor of the Year while serving at Naval Computer and Telecommunications Station in Sicily.

Arnold's nomination was for the majority of her time at Naval Communications Station Far East (NCTS FE) conducting Periodic Training and Assist visits to eliminate short-term problems that hampered shipboard mission accomplishment or out of area temporary additional duty, across five geographically dispersed countries that provided vital Communications Security (COMSEC) Material training to more than 800 personnel, including Commanding Officers, EKMS managers and CMS users. She led, mentored and trained Electronic Key Management System (EKMS) teams, managers and alternates from the Department of the Navy (DoN), United States Marine Corps (USMC), United States Coast Guard (USCG), and Military Sealift Command (MSC). Arnold championed and instituted the redevelopment of an aggressive training regimen for EKMS inspectors in the Seventh Fleet Area of Responsibility, which increased overall readiness and flexibility.

" ... I have been blessed to always have had senior leaders that took me under their wing in every assignment during my 18 years of Naval Service. In my personal life, my grandmothers taught me strength through adversity."

Through practical experience and training, she qualified other EKMS inspectors and provided them with the proper knowledge of policy, procedures, and training techniques.

"I have had strong leadership in my career," said Arnold, "and I have been blessed to always have had senior leaders that took me under their wing in every assignment during my 18 years of Naval Service. In my personal life, my grandmothers taught me strength through adversity."

As the NCTS FE Enlisted Information Dominance Warfare Specialist (EIDWS) Board Chairman, Arnold set the tone for career progression and personal development of Sailors. Her firm but fair 'take charge' approach resulted in 100% active participation in mentorship relationships. She provided oversight to protégés as well as the widely dispersed detachments and displayed a sincere concern for Sailors and officers, implemented a new system of mentor assignment within the command, and actively scheduled and provided personal and professional guidance resulting in a morale boost and readiness.

"I believe in Sailors ALWAYS," said Arnold, "and I am committed to developing Sailors and enforcing standards; remaining responsive, being aligned and well-connected to both leadership and Sailors."

The board received over 140 nominations and convened over two days. Awards were presented at the Joint Women's Leadership Conference in Washington, DC, during Women's History Month.

Although not selected, the impact and magnitude of the nomination was not lost on Arnold.

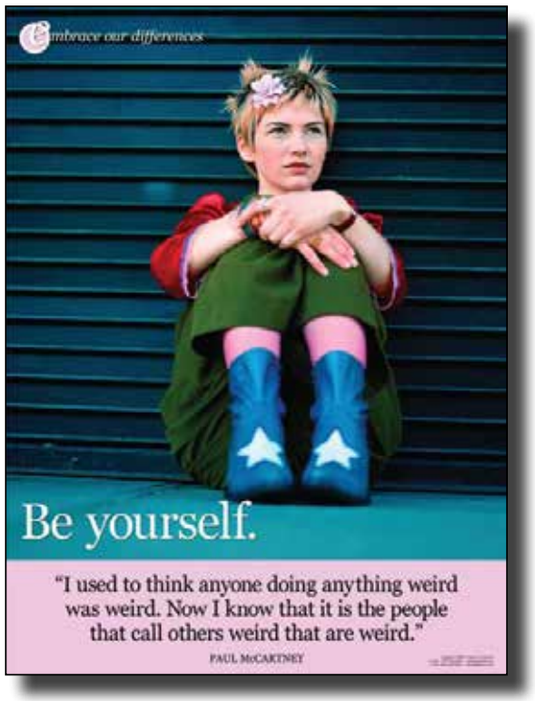
"I am honored and humbled that the Chain of Command chose to recognize my contributions to the Command and the Navy," said Arnold.

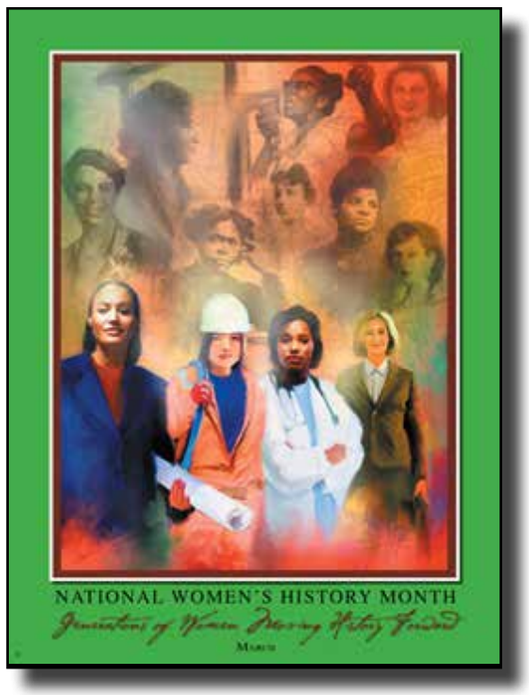
Official U.S. Navy Photo

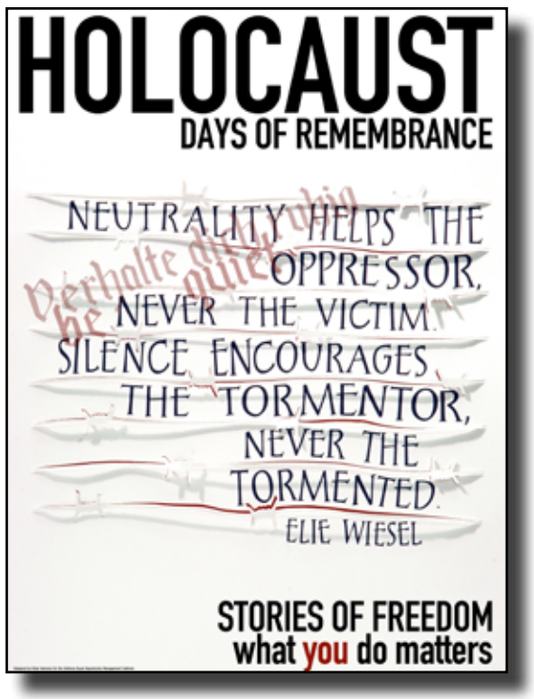
ITC Dawn Arnold

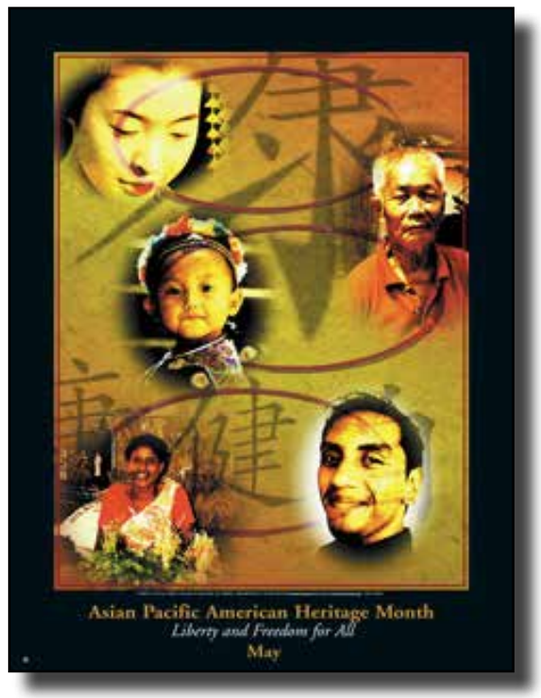
Photos by Robin Hicks

(Clockwise from left) Elena Barr Baum, Director, Holocaust Commission United Jewish Federation of Tidewater addresses the CYBERFOR audience during the Holocaust Remembrance Day/Days of Remembrance Program on May 2. **(Above)** The program featured a video of Holocaust survivor Hans Loewenbach from a larger program called "What We Carry". **(Right top)** Barr Baum points out an artist created suitcase full of replicas of the survivors' artifacts and mementos. **(Right Bottom)** A Sailor closely inspects the afore mentioned display.









NETWARCOM

Remembers One of Its Own

Roger D. Williams
(September 6, 1958 - April 8, 2013)

Roger D. Williams, 54, unexpectedly passed away April 8 at his Chesapeake, VA, residence.

Born in Indiana, he was the son of the late Charles and Dorothy (Kelsey) Williams. He was a graduate of East Palestine High School.

Williams enlisted in the Delayed Entry Program in 1976 at the age of 17 and entered active duty the week following his 18th birthday. After four and a half years as an enlisted Sailor, he earned his commission in 1981 and achieved the rank of commander.

While in the Navy he served in Misawa Japan, Guam, Pearl Harbor and Subic Bay. In 2003 he retired from Fleet Information Warfare Center, Norfolk, VA, at the rank of commander.

He joined the civil service in 2005 and performed superbly for Navy Cyber Forces' manpower and later as the administrative officer for Global Network Operations Command and Naval Network Warfare Command (NETWARCOM).

"I can say first hand that he was an extremely competent, dedicated and loyal employee," said CAPT John Chandler, commanding officer, NETWARCOM. "He was truly one of our best and will be missed by all of us here in 'Team Cyber'".

Williams was baptized and confirmed in the Catholic Church on Mar. 31, 2002. He was a devout member of Prince of Peace Catholic Church in Chesapeake, VA. He was a dutiful volunteer of Habitat for Humanity and a proud member of the Knights of Columbus.

Williams is survived by his wife of 27 years, Marivic Williams; his 22-year-old daughter, Kimberly Williams; two brothers, Bruce and Timothy Williams; a sister, Pamela Dunn; and mother-in-law, Mamerta Cuartero; as well as 30 nieces and nephews and many wonderful in-laws.

Memorial donations may be made in his name to Prince of Peace Catholic Church.

LOOK FOR US ON THE WEB

www.cyberfor.navy.mil

or

www.facebook.com/USNavyCyberForces